Technical Report **1748**
29 August 1997

# Network Planning Guidebook for Small Naval Shore Facilities

Version 2.0

**Prepared for:**
Department of the Navy Chief Information Officer,
(DoN CIO), Office of the Secretary of the Navy

**Prepared by:**
Networking Integrated Product Team (IPT) and the
Department of the Navy's Information Network
Program Office (DoN INPO)

Approved for public release; distribution is unlimited.

Naval Command, Control and Ocean Surveillance Center
RDT&E Division, San Diego, CA 92152–5001

# CONTENTS

## FIGURES

## TABLES

## APPENDICES

# 1. INTRODUCTION

The purpose of this document is to provide Navy organizations (500 users or less) with a consolidated reference to assist in determining if automation will improve their business practices. If it is determined that a Local Area Network (LAN) is required, this document provides information on contract vehicles and provides a consolidated reference for the organization's Automated Data Processing representative.

The planning and installation of a LAN is very complex and expensive, requiring the support of an expert. This document is not intended to be a "how to" book for designing and installing a LAN.

Networks are an integral part of Information Management (IM) systems. Cost-effective IM solutions can be realized through the use of available Commercial Off-the-Shelf (COTS) products. The use of COTS products designed to meet the requirements of Information Technology (IT) standards promotes the interoperability and compatibility of information systems.

This document provides guidance in technology and product selection to assist personnel tasked with the coordination, planning, and installation oversight of an organization network to achieve these objectives.

# 2. SCOPE AND CAUTIONS

The intent of this guide is to assist the organization's technical person and/or a small team, who do not possess specific networking experience, in the process of determining the need for a LAN and planning a network tailored to the requirements of the organization. This guide is intended to be used by organizations of 500 or fewer users located within a small environment where LAN technology can be effectively employed in the support of various applications. The LAN should use standards-based COTS components to the maximum extent possible. This document provides direction for defining requirements, configuring the network with the assistance of contractor support, and selecting products so those requirements will be satisfied. In addition, specific methods and resources are identified for procuring and installing equipment.

The guidance provided in this document is structured to ensure that users will be compliant with ongoing naval programs, such as the Base Level Information Infrastructure (BLII) Program, and with various claimant initiatives, such as Information Technology for the 21st Century (IT-21). The guidelines address construction of non-stovepiped data networks (in other words, data networks that will interoperate with other Department of the Navy (DoN) data networks). This guide does not address switched voice networks (telephone services), although the self-help data network infrastructure created by following these guidelines will interoperate with switched voice networks.

While the level of expertise of the readers of this document could vary from complete novice, in all or some areas, to an expert in many areas, no previous network background on the part of the reader is assumed. Information included should be of value to personnel with various levels of experience. Familiarity with the use of computers as well as some knowledge of hardware and software components is assumed.

Because this document is a guide, and not a specification or directive, it does not dictate requirements for implementation. Conformance to existing and emerging standards will be achieved by following the recommendations. Guidelines provided herein are in accordance with commercial standards, advertised Navy direction, and good engineering practices. **References and instructional information are provided in bold type to aid the reader. References are provided in the text when further information is available.** Resources are available where the reader or planner will be able to obtain assistance or consultation services should difficulties be encountered or when a "sanity check" is desired during the process. **These resources appear in the text as appropriate, and a summarized list is provided in Section 4. Section 5 provides a list of references and where they can be obtained.**

**Important DoD/DoN references to consult are:**

**"Technical Architecture Framework for Information Management (TAFIM)," Volume 3, March 1997, and The Joint Technical Architecture (JTA), Version 1.0, August 1996.**

**The "Defense Information Infrastructure Common Operationing Environment (DII COE)" documents, including the DII COE Security Checklists.**

**"Department of the Navy Automatic Data Processing Security Program (OPNAVIST 5239.1A)," August 1982**

**"Department of the Navy Information Systems Security (INFOSEC) Program (SECNAVIST 5239.3)," 14 July 1995**

# 3. NETWORK REQUIREMENTS ASSESSMENT

This section is intended to provide guidance in the assessment of the organization's networking requirements. This will be done via a step-by-step walk-through of the process. As terms are introduced, they will be defined and a brief tutorial will be presented as to how they apply to a network. Pointers are also provided for additional information.

Good books on networks are available in libraries and bookstores that supplement the information provided. Information may also be obtained from equipment vendors. However, caution must be taken when reading this material as it may be slanted toward their products. Solutions may also be proprietary and may not provide interoperability with other vendors' products. Unfortunately, it is sometimes too easy to be locked into one vendor's line of products.

**One book to start with is "Networking for Dummies," which contains information on various aspects of networks. Chapters 9 through 11, in particular, are recommended.**

**A specific implementation for setting up anonymous File Transfer Protocol (FTP) with the standard UNIX FTP server is described in "Practical UNIX and Internet Security," 2nd Edition, O'Reilly and Associates, pp. 491-493.**

**A specific implementation for setting up Domain Name Service (DNS) is described in "Building Internet Firewalls," O'Reilly and Associates, pp. 278-296.**

Readers are also encouraged to learn about the Internet. The Internet has a wealth of material on all aspects of networks. Information is available for online reading as well as for downloading via a Web Browser for off-line review. Connectivity can be made to the Internet by subscribing to a local Internet Service Provider (ISP) for approximately $20/month/user. A Personal Computer (PC), running a Windows operating system, with a modem and a phone line is all that is required. It is recommended that the organization select an ISP that does not charge for usage by the minute.

**The Internet Engineering Task Force (IETF) puts out a series of documents called "Request for Comments (RFCs)." RFCs are the mechanism used by the IETF to issue documents that have gone through a review process and are classified as proposed, required, experimental, or optional standards. Documents still in the review process are called "Internet Drafts." Most of the items discussed in this document are defined by RFCs. RFCs are a good source for information. The IETF standards referenced herein define operational components.**

## 3.1 A QUICK LOOK AT NETWORKS

Networks inherently employ a variety of components. The interconnection of all computers and other devices forms the network or organization infrastructure. Figure 1 shows an elementary depiction of the interconnection of network components.

Definitions of components shown in the figure are presented below along with other components that are not shown. Section 3.2 provides functional descriptions of the components.

### 3.1.1 Basic Components

#### *3.1.1.1 Computers, Operating Systems, and Applications*

A **computer** on your network could be an IBM clone, a Macintosh, or a workstation.

The computer requires an **operating system,** which could be DOS, Windows NT, System7, UNIX, or another type.

Personnel in the organization use **applications** on the computers to communicate information, via the network, among themselves and with others outside the organization. Electronic mail (E-mail) is the most commonly used communications application.

#### *3.1.1.2 Media Interface*

Each computer requires an interface to the media. This interface is commonly called **a Network Interface Card (NIC).**

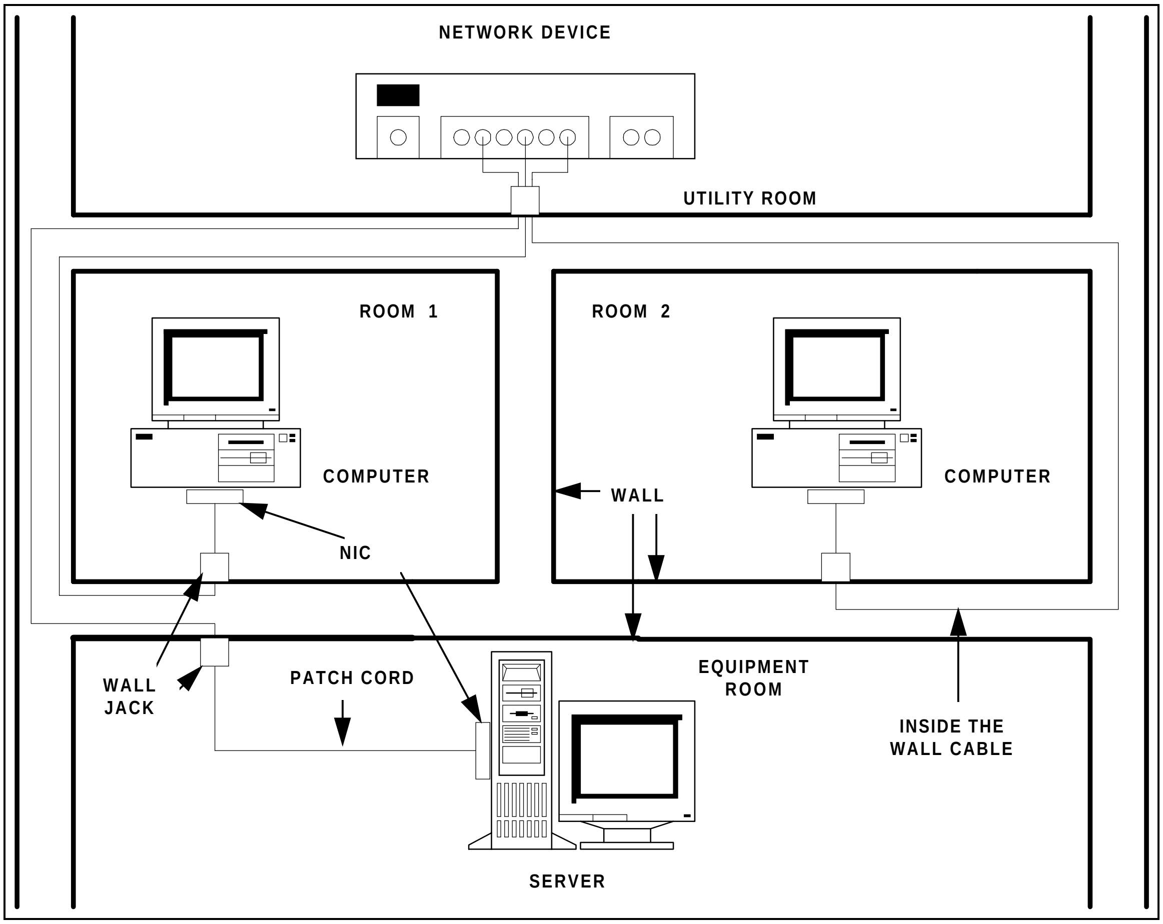


**Figure 1. Basic Network Component Interconnectivity.**

### *3.1.1.3 Media*

A media or cabling is required to interconnect the computers. The media could be copper or fiber cable or a combination of both. Common types of copper cables are coaxial and twisted pair.

A **patch cord** connects each computer's **NIC** to a **wall outlet**. The wall outlet looks similar to the telephone jack, only larger. The "**behind the wall**" media connects the wall outlet to network devices and then to other computers. Behind the wall, wiring may be run above the overhead or under the floor.

Note: Power cables for these components are not shown in Figure 1.

### 3.1.2 Network Components

### 3.1.3 Interconnecting Devices

These components interconnect sets or groups of computers. Figure 1 shows a hub connecting the computers and the server. In actuality, this device could be a **hub, bridge, router,** or **switch.** Each has a different role in connecting devices depending on the functionality required.

#### *3.1.3.1 Servers*

Servers support the applications running on the network. Common roles are **file, mail, name,** and **address servers.**

## *3.2* NETWORK BASICS

A network enables the exchange of information in electronic form among individuals, groups, or organizations. The network provides the communication mechanism between connected users. This is achieved through a combination of hardware and software. Computers and peripheral devices are interconnected via a physical medium, such as copper cables and/or fiber-optic cables. Wireless communication technology is not addressed in this document.

Building a network is a process of selecting cost-effective components to meet the requirements of the users. More than one option is normally available for these components. Different technology choices can be made to solve the same problem. Making the right choice can be difficult because technology is advancing at a rapid pace. Competition among vendors should reduce costs. At the same time, there is a race to increase performance that typically increases costs. Thus, it is important to understand the requirements of the organization so that valid technology tradeoffs can be made to arrive at a cost-effective solution.

### 3.2.1 Which Category of Network?

The category of network employed is distinguished by the geographical coverage of the network. A LAN is restricted in coverage to within a small geographical area, such as might be associated with a workgroup. The members of the workgroup may be co-located in a single building, or in a small number of buildings in close proximity. In the context of this guidebook, the network will be limited to connecting 500 or fewer users located within a building, or a group of buildings within a radius of 0.5 mile.

Several LANs can be interconnected within a building or buildings to extend connectivity and reduce contention for resources.

A Campus Area Network (CAN) would cover a larger geographical area than a LAN, on the order of a few miles.

A Metropolitan Area Network (MAN) would cover an area the size of a small city.

A Wide Area Network (WAN) provides connection between sites in diverse locations.

### 3.2.2 What Can I Do with a Network?

A LAN allows resources to be shared. For example, a printer can be set up as a shared resource that computers on the network can access. Thus, each user does not need a dedicated printer co-located with his/her computer but can share with other users. The organization’s printer can thus be of higher quality and still be less costly than a quantity of dedicated printers.

Similarly, the LAN allows files to be shared. Common files used by a group of users can be installed on a file server. This frees up space on each user’s hard drive. The user can download the required file when it is needed. This process can be extended to programs as well. In this case, for example, a copy of a word processing program can be stored on a server. A user would download the program when he/she needs to use it or use his/her computer as a terminal while interacting with the program on the server. Since each user does not require permanent storage of the program on a local computer, costs are reduced.

Software commonly called “groupware” allows users to collaborate on documents. Workgroup users can observe the same annotations attached to documents if they are using common applications to view the documents.

The LAN can be connected to the Internet, thereby extending coverage and the functions of the applications beyond the organizational level.

#### *3.2.2.1 Capabilities*

As a minimum, the network should support the following applications:

***Electronic Mail (E-mail).*** E-mail allows users to send and receive messages between members of the organization and with individuals outside the organization.

E-mail capability permits a user to selectively send messages to another user, or users. A message consists of a header (addressing information), the message body, and/or may include an attachment or attachments. An attachment is a file, for example a form or report generated on a word processor, which is added to the message. The attachment is typically encoded at the sending end and decoded at the receiving end. This coding process preserves characters or commands that the formatted file contains.

***Web Access.*** Web access allows users to access established “home pages” and view and/or download presented information.

Home pages are established by organizations and/or individuals to advertise and promote their capabilities and to provide information that can be viewed online or downloaded for later viewing. With connection to the Internet, users will be able to access Navy, DoD, other government, as well as other home pages residing on the Internet. Conversely, when the local organization establishes its home page, it will be accessible to the same wide audience of viewers. Precautions can be taken to restrict access to items appropriate for the particular viewer.

The World Wide Web (WWW) has achieved wide popularity. The WWW can be considered a global distributed database. Universal Resource Locators (URLs) identify server programs running on remote nodes. The Hypertext Transfer Protocol (http) is used with these applications. Information may be in the form of text, sound, graphics, or multimedia. This information can be “viewed” online or downloaded as a file for later “viewing.” (The quotations are used since information in the form of sound is not really viewable by sight. “Sound” here refers to audio information, whether verbal or music based.)

***File Transfer.*** File Transfer allows users to send files to designated file servers and to access and receive files from these servers.

File transfer is useful in situations where information is intended for a selected set of individuals where access to the information is restricted. File transfer is also required in cases where E-mail systems limit the size of message attachments.

Software used for providing communications over the network normally provides the commonly used File Transfer Protocol (FTP). A protocol is merely the procedure or set of rules that must be followed for proper communication to be established, maintained, and terminated on completion. Web browsers also support file transfers. FTP allows a user to transfer a file to or from a remote server. **FTP is defined in RFC 959.**

### *3.2.2.2 How Do I Use These Applications?*

**Applications for communicating over the LAN have some common aspects. These are described below.**

***Communication Protocols.*** Protocols provide the procedures or rules that must be followed in order to communicate across the network. As part of these procedures, the protocol provides a formal description of the message formats. The most commonly used communication protocols are the Internet Transport Control Protocol/Internet Protocol (TCP/IP). TCP uses the services of IP for the transfer of user-generated information. IP is responsible for the delivery of data over the particular hardware and media used in the network. TCP and IP are software and are typically packaged together. A simpler, less reliable transport protocol, Unit Datagram Protocol (UDP), is also included in the package. Implementations also provide useful utilities or tools that are commonly used, for example, for determining connectivity (ping), or for locating other users (finger). **TCP and IP are defined in RFC 793 and RFC 792, respectively, while UDP is defined in RFC 768. A tutorial on TCP/IP is provided in RFC 1180.**

***Addressing.*** For a message to reach its recipient, the address of the message recipient must be provided. The communication protocols use this address to locate the recipient and determine the path between the sender and recipient. When IP addresses are used to determine a path, the path is called a route. The address of the sender is also required. This allows the recipient to respond to a message.

Domain naming, and its most visible component, the Domain Name Server (DNS), is critical to the operation of the network. DNS is also used on the Internet. DNS is effectively a database of addresses arranged in a hierarchy (an inverted tree) called “domain names.” DNS is an interconnected set of name servers called the “domain name hierarchy.” No two organizations can have the same domain names or address. The domain name is used to identify and locate computers connected to the network. **Documentation on DNS is provided in RFC 1034 and RFC 1035.**

**Examples of top-level domain names used in the U.S. are:**

| | |
|---|---|
| **com** | **commercial** |
| **edu** | **educational** |
| **gov** | **U.S. government** |
| **mil** | **U.S. military** |
| **net** | **network providers** |
| **org** | **organizations (non-profit)** |

**An example of a host name is:**

**hostn.hq.navy.mil**

**where:**

**"mil" is the top-level domain,**
**"navy" is the second-level domain,**
**"hq" is the sub-domain, in this case headquarters for the Navy,**
**"hostn" is the organization designation for a particular server, and,**
**the period, or dot, is used to separate portions of the address.**

Not all domain names will have a host name and subdomain.

To make use of domain names, they must be converted from user-friendly textual host names into numerical 32-bit IP addresses. Every computer on the network must have a numerical IP address. This address must be registered into a DNS on the network. Once listed in the database, the host can be located and communications can be initiated.

The LAN must be provided with a DNS to resolve addresses and routes within the LAN and external to it. The local DNS must be able to communicate with DNSs located beyond the LAN boundaries.

**The particular requirements for each capability are described below:**

***E-mail.*** To provide E-mail capability, each computer must have an installed E-mail software package. A number of such programs are available with a variety of features**.** The E-mail package you use must be compliant with the Defense Message System (DMS) and should be compatible with the Internet Simple Mail Transfer Protocol (SMTP). It should also have Multipurpose Internet Mail Extensions (MIME) capability so that attachments can be appended to the message. **SMTP is defined by RFC 821. MIME is defined in RFC 1522.**

SMTP is the Internet's standard for host-to-host mail transport protocol. Since it was the first E-mail service, and the Internet has enjoyed wide usage, E-mail packages for LAN-based computers are designed to be compatible with SMTP.

Most E-mail programs employ a mail server to act as an electronic post office. Messages are stored on the server until they are delivered to the recipient. The server functioning as the mail server may also provide other services such as file storage.

One computer with the NT operating system can be set up to provide the function of the mail and file server and also to provide the DNS capability.

Using a mail server offers the advantage of off-loading stored messages from the desktop computers and off-loading some processing resources to the server. Also, the server will still receive messages when the desktop computers are down for maintenance. The user can initiate the process of downloading messages from the server. The server acts as a gateway between the organization and the rest of the world. Organization users must be registered on the server.

**In accordance with DoD policy, the Defense Information System Agency's (DISA) Defense Messaging System (DMS), which consists of an X.400 E-mail Service and an X.500 Directory Service, will be required by 1999 (see OASD(C3I) Memo dtd 13 Oct 92 and OASD(C3I) Memo dtd 9 Mar 95 at DISA DMS website at URL:**

**http://www.disa.mil/D2/dms/docs/progovw/toc110.htm)**

**(Also see the Navy's DMS Website at URL:**

**http://www.spawar.navy.mil/~DMS/index.html.)**

**There are DMS-certified products available. Among them are Microsoft Exchange and Lotus Notes products for E-mail. (See Website at URL http://www.disa.mil/D2/dms/press2.htm and Website at URL http://www.part.net/itec/itec.htm for ITEC contract information.) CINCPACFLT and CINCLANTFLT have also established standards for their claimants under the IT-21 initiative (reference CINCPACFLT Administrative Message dtg 300944Z Mar 97, Subject: Information Technology for the 21st Century). For further information, contact the Department of the Navy DMS Program Office (SPAWAR PMW-152).**

***Web Access.*** Web access requires that computers needing this capability be configured with a Web Browser. **Commonly used Web Browsers are:**

**Mosiac**

**Netscape Navigator®**

**Microsoft® Internet Explorer.**

Most browsers offer similar capabilities. Users may recommend one over the other based on familiarity and personal preferences.

**URLs are in the form of**

**http://www.hq.navy.mil/page.html**

**where:**

**"http://" is the Hypertext Transfer Protocol prefix,**

**"www" is for World Wide Web,**

**"hq" designates the agency or organization element, and is not always required,**

**"navy" designates the agency or organization,**

**“mil” designates the domain.**

**Taken together, www.hq.navy.mil defines the address of a particular host belonging to Navy Headquarters. This is referred to as a Web Site. The dot, or period, is used to separate portions of the address.**

**A specific page on the host is designated by “page.html,” with “html” referring to the Hypertext Mark-up Language, the language used in constructing pages for Web browsing. If “page.html” is not specified, the server will often default to an index file.**

**Once the visitor has accessed the Web Site, he/she can then jump to other pages on the host or jump to other sites linked from the HQ server .**

***FTP.*** FTP is the commonly used file transfer protocol typically packaged with TCP/IP. To invoke it, the user uses the following procedure. Refer to RFC 959 for additional information.

**ftp hostname.thirdleveldomain.secondleveldomain.firstleveldomain.**

**The user will be prompted for user identification and password.**

One of two cases will arise, depending on the level of access for the user.

**Case 1: User is listed with access privilege.** In this case, a file server has been designated by the organization for the storage of commonly used files or for files that exceed the capability of the E-mail system.

**The user should enter his/her assigned user id for this host.**

**The user should enter his/her password for this host.**

**Case 2: User is not listed with access privilege.** Organizations typically have a host available for general public access.

**The user should enter his/her assigned user id, including host address.**

**The user should enter “anonymous” as the password. (In some cases, “guest” is used as the password.)**

At this point, the user should be registered on the host to either upload a file or read a file on the host or download a file to his/her desktop computer.

### 3.2.3 What About Performance?

The performance required of the network will depend on the performance of the computers that are connected, the applications that are on these machines (computers or servers), the number of machines (computers or servers), and the method of interconnecting them. If one is constrained to the use of computers that the organization already owns, then performance could be limited by the speed of these computers, especially if they are an older vintage. Newer computers with fast Pentium processors will allow the organization to benefit from the performance offered by the speed of the LAN.

As a rule, the fewer the number of devices on a LAN segment, the better will be the performance. The computers on the LAN segment compete for use of the shared media. A segment is the smallest piece of a network on which the computers can exchange information without the intervention of an intelligent network device.

Another good rule is to try to use LAN segments for groups of users, that is, users whom communicate amongst themselves and/or use common services. Communication with users or services outside the group can be established via the use of intelligent network devices that interconnect LAN segments to form a larger LAN.

### 3.2.4 What Components are Required in a LAN?

The answer can differ with each situation. Some components are required in most or all situations, while others may be required in special or unique situations. **This document will point readers in the direction of Ethernet LAN configurations.** Ethernet has been around for several years and is widely supported. Prices are therefore relatively low compared with other technologies. Additionally, it offers several options relative to performance.

**A good source for tutorial information on networks is the Web Site for “Network Computing” magazine. The URL for this site is:**

**http://techweb.cmp.com/nc/netdesign/series.htm**

**The magazine itself is issued monthly. Free subscriptions to the magazine are offered. Address and telephone information is provided in Section 5.1.**

Basic Ethernet operates at 10 Megabits per second (Mbps). A Megabit is 1 million bits. Ethernet in one form or another has been around since the late 1970s. A 10 Megabits per second (Mbps) version has been **standardized by the Institute of Electrical and Electronics Engineers (IEEE) as IEEE 802.3 in the early 1980s.** Subsequently, other versions of Ethernet have been defined (see Section 3.1.4.2). Specifications are available from the IEEE. **Ethernet is also defined in RFC 894.**

#### *3.2.4.1 Configurations*

The linear bus configuration, shown in Figure 2, is one of the earliest configurations, and is still common. The linear bus is an example of a LAN segment. Each computer is attached to the bus via a stub cable. The media used was coaxial cable. The stub cable attaches to the main cable via a connector, forming a tap on the base. The cumulative effects of the taps and bus length results in loss of signal strength as it travels down the main cable. The bandwidth of the bus is shared by all the attached computers.

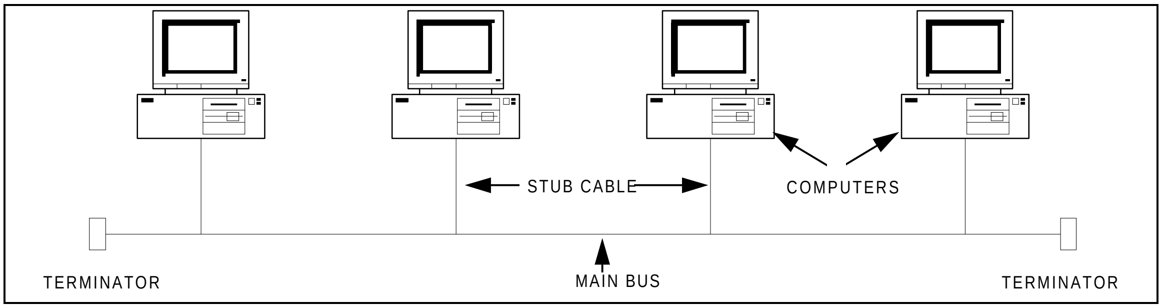


**Figure 2. Linear Bus Configuration.**

With the advancement of LAN products, other configurations are displacing the linear bus configuration. Figure 3 shows a generic hub configuration for the same set of computers as shown in the linear bus example. The hub serves as a distribution point for the interconnecting cable to the computers. While the configuration is physically a star, it behaves electrically as a linear bus. Each device is connected to a port on the hub, which acts as a repeater. Signals are regenerated before being sent to the devices. The interconnection cabling for each computer can be shorter in length and, since taps are not present, the cable does not have to be of the same high quality. Therefore, cheaper media can be used inside a small building.

Each computer must be provided with an Ethernet-compatible Network Interface Card (NIC). The NIC, which may be on the computer motherboard, provides the network functions for the computer and the connector to which the network cable is attached. Each NIC is provided with a globally unique hardware address by the vendor. Copper or fiber cabling may be used for the connections internal to buildings and between buildings. Current practice is to run LAN cabling in a manner similar to the wiring provided in buildings for telephone use. Telephone wiring is distributed from wiring closets to the individual telephones. Similarly, centralized wiring simplifies the LAN administration and maintenance requirements by enabling all network modifications, additions, deletions, and relocations, to be accomplished in the wiring closet.

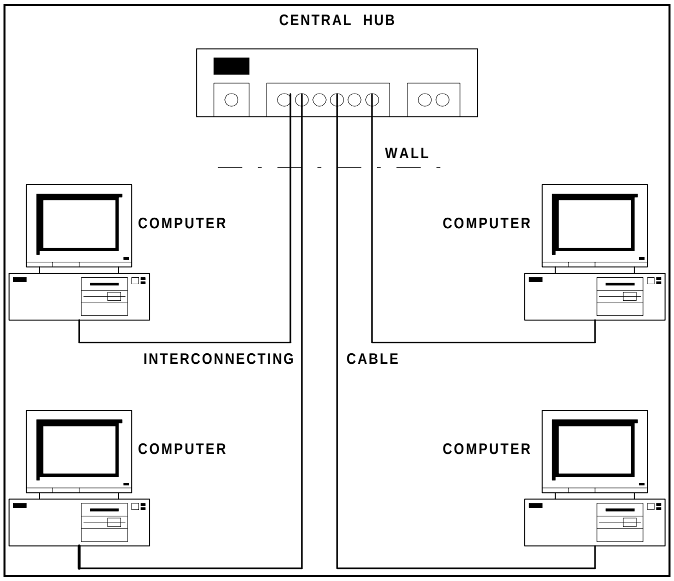


**Figure 3. Basic Star Configuration.**

The hub is a simple interconnecting device with minimum functionality. It is not an intelligent device connecting devices on the same LAN segment. The hub can be used to connect strings of stations by connecting a linear bus to a properly configured port. Hubs can, in turn, be interconnected via a linear bus configuration or cascaded by point-to-point connections. These approaches are illustrated in Figures 4 and 5, respectively, for the installation of a LAN in a multi-floor building.

These figures show the hub connecting stations via a LAN on the first floor of the building and via point-to-point connections on the other two floors. A server is also shown on the second floor.

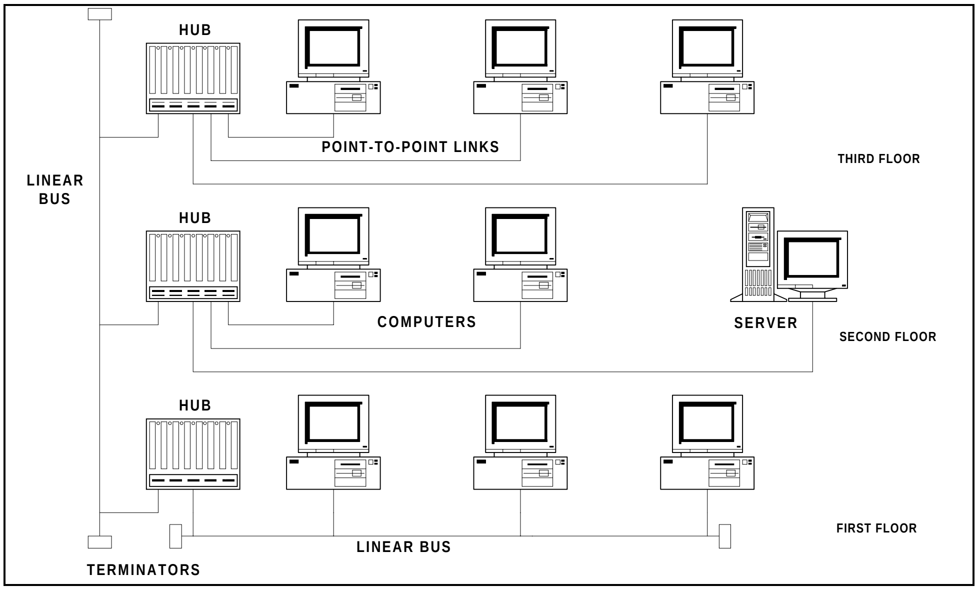


**Figure 4. Linking Hubs via Linear Bus.**

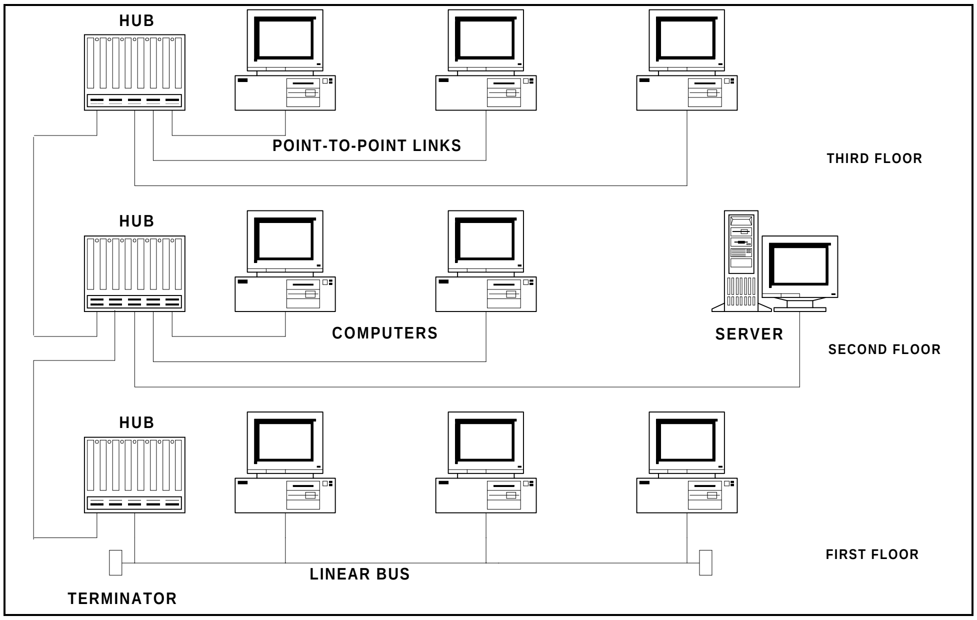


**Figure 5. Cascaded Hubs.**

This process cannot be extended indefinitely. All stations interconnected with hubs are on the same LAN segment. Traffic conditions will, at some point, start to saturate the LAN, and traffic will approach the capacity of the LAN. It will become necessary to partition the network into segments.

**Three good rules of thumb to follow to provide adequate performance to the users of the LAN are:**

1. **Limit the number of stations on a single segment to less than 100.**
2. **Traffic on a single segment should obey, as closely as possible, the 80/20 rule, where 80% of the traffic on a single LAN segment is between stations on the segment, and the other 20% is for stations on other LAN segments.**
3. **Keep traffic on a single segment to less than 35% of the capacity of the LAN. This means that for Ethernet LANs, which operate at 10 Mbps, the operational traffic should be less than 3.5 Mbps. This allows for some growth, either for more data-intensive applications or for more users, or both.**

### *3.2.4.2 Interconnecting Devices*

Intelligent devices are required to partition the network into segments to obtain the performance required.

***Bridge.*** A bridge is used to connect two or more similar segments together. A LAN that uses a bridge is called an extended LAN. A bridge has two purposes. The first is to extend the length and number of stations that a segment can support. Secondly, the bridge reduces overall traffic flow by only passing data packets that are not destined for a hardware address on a local segment. A bridge is considered an intelligent device. Packet-forwarding decisions are made on the basis of hardware addresses.

***Router.*** A router is used to connect two or more segments. The segments may be similar or dissimilar. A LAN that uses a router is called an internet or subnet. Routers perform an inter-networking function. Subnetworks are associated with an assigned port on a router. Packet-forwarding decisions are made on the basis of the IP Address and information stored in routing tables. Hardware addresses have only local significance to a router, whereas routing information is globally significant**.**

Both bridges and routers are data-forwarding devices, transferring packets between LAN segments or networks, respectively. They allow for the design and operation of more efficient networks. Internal tables are employed in the packet-forwarding decision process. This process takes time and therefore adds to the latency of the network.

These traditional devices still have their uses; however, due to their limitations, developing trends in increasing file sizes, increased productivity of LAN workgroups, and Web usage, these devices are being supplanted by switches.

***Switch.*** Switching is a technology that facilitates the reduction of the number of stations per segment. This improves performance in that it reduces contention for the shared media. Thus, switching has come to mean an architecture where any incoming traffic can be redirected to any outgoing port with relatively little concern for traffic loss or congestion. Switches provide a means to separate collision domains and to allocate bandwidth to a user or a set of users. The bandwidth available in a well-designed switch is the cumulative bandwidth of all its ports.

The method by which a switch determines the path on which to direct traffic could be based on the use of bridging or router information. A switch allows information on any incoming port to be passed to any outgoing port. Traffic between different incoming ports can be passed to idle outgoing ports simultaneously.

Switches also offer the advantage of being able to accommodate different data rates on different ports. Ports can be provided with different speed capabilities. Thus, a server with high utilization can be provided with more bandwidth than segments with lower requirements. Figure 6 shows how a LAN could be installed within and between buildings.

Switches are available in different sizes and with different capacities and configurations. The latter two items are functions of the modules installed into the switch cabinet. These modules are the switch ports. Switches can be cascaded. Thus, if dictated by loading conditions, any of the hubs shown in the figure could be replaced by a switch configured to provide the level of service required.

**Note the conduit between buildings. Before calling the backhoe operator to dig a trench, check with the base Public Works to determine if there is a conduit already in place that could be used. It’s possible that there could even be spare (unused) fiber in the conduit.**

**EIA/TIA 568, the Commercial Building Standard, defines fiber cable as the cable of choice for connections between buildings.**

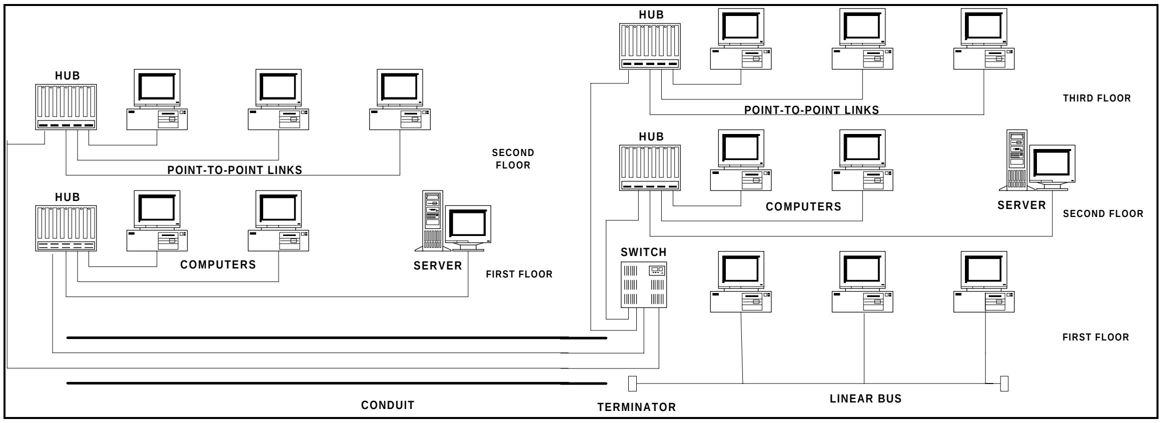


**Figure 6. Representative Inter-Building LAN Configuration.**

The components of the LAN are interconnected via copper or fiber media. Network interconnecting devices such as routers or switches physically isolate devices on one port from devices on other ports. Therefore it is possible to mix media, that is, to use different media or different size media in the network. Fiber can be attached to one or more ports while copper of different types or dimensions can be attached to other ports.

**Table 1 lists the Ethernet family of standards.** Specifications are available from the IEEE.

**Table 1. IEEE 802.3/Ethernet Family of Standards.**

| **STANDARD NUMBER** | IEEE 802.3 | IEEE 802.3a | IEEE 802.3i | IEEE 802,3F |
|---|---|---|---|---|
| **IEEE NAME** | 10 Base 5 | 10 Base 2 | 10 Base T | 10 Base FL |
| **MEDIA TYPE** | RG-8 | RG-58 | Unshielded Twisted Pair | Fiber |
| **OTHER NAME** | Thick Net | Thin Net | UTP | Ethernet, Fiber |

The “5” in 10 Base 5 refers to a segment length of 500 meters, the length of the LAN cable. Larger cable diameter permits longer cable lengths; thus, Thick Net permits cable lengths of 500 meters, without repeaters. Repeaters should be avoided. Thin Net is limited to 200-meter cable lengths and consequently is used only in small office environments.

Thick Net and Thin Net Ethernets are configured as a linear bus where network stations tap into the cable at points along the cable. The taps and the cable lengths contribute to transmission losses that attenuate the signal as it progresses down the cable. Thick Net and Thin Net employ coaxial (coax) cables where the outer conductor acts as a shield with respect to Electro-Magnetic Interference (EMI) generated by sources external to, but close to, the cable. Thick Net has largely been superseded by fiber optics and Thin Net in new installations. Unshielded Twisted Pair (UTP) cable, as the name implies, has no shield. The characteristics of UTP are such that higher losses are encountered per linear foot of cable. UTP also comes in different grades or categories that affect the noise reduction qualities of the cable with respect to EMI. UTP Category (CAT) -

5 cable is recommended for 10 Base T with wire sizes of 22 to 26 American Wire Gauge. It should be noted that CAT-5 cable must be installed with more care than ordinary telephone cable to preserve its electrical characteristics.

UTP is cheaper than Thick Net and Thin Net cable. In many cases this cable is available as building wire typically used for telephone connection. The configuration of Ethernet with UTP is a star with centralized hub devices in telephone wiring closets. UTP is connected in a point-to-point manner between the computer and network device. Maximum length is limited to 100 meters.

Fiber-optic cabling can be used with Ethernet. However, due to the characteristics of the media and coupling mechanisms, there is no fiber-optic tap equivalent to the copper cable tap. Therefore, other mechanisms such as optical star couplers are used. The sum of cable lengths between any two stations cannot exceed the 500-meter segment length. It is possible to run at a data rate of 100 Mbps at a distance of more than 1 mile with fiber optics. Thus, fiber between buildings is a good choice. Fiber optics offers security benefits as well. Light is trapped inside the fiber so that there is no external radiation. The Ethernet standard allows a variety of optical fiber sizes; however, the Navy has adopted the 62.5/125 micrometer fiber as a shipboard standard. (The first number refers to the core diameter, the second number refers to the overall fiber diameter – fiber plus cladding.) This fiber is widely used in commercial applications and is the recommended fiber type for the networks discussed in this document.

Light travels down the core of the fiber. The cladding that surrounds the core restricts light propagation to the core itself. Fiber is a fragile media. Similar precautions must be taken with fiber as with UTP during installation, as described below.

Fiber cables are available with multiple fibers. Internal strength members are provided within the cable. External protection around the cable is added as well. In military applications involving secure information or information that should not be disclosed to the public, special protective covering is used in installations external to buildings and in secure spaces.

The protocol or procedure employed by all versions of Ethernet to access the cable and transmit information uses parameters that are functions of the 500-meter segment length. The protocol, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a “listen before sending” and “listen while sending” protocol. The CSMA/CD protocol is referred to as a contentious protocol since users on the media must contend for access to the media. This protocol is not orderly, unlike some other LAN protocols where users can access the media in a specified order.

A station (computer or other device) that has information to transmit must listen for a minimum period of time for quiet condition on the cable prior to sending the information or message. This minimum time, 9.6 microseconds, corresponds to the maximum two-way (up and back) delay the cable provides due to the laws of physics. (A microsecond is 1 millionth of a second.) After detecting the required quiet condition, the sending station must listen to the transmitted message. Due to the delay of the cable, it is possible that another station sensed the quiet state and also started transmission of a message. Therefore, the two messages will collide, invalidating the data. Each station would then have to revert to sensing the quiet condition. A method, or algorithm, is provided such that the two stations attempt to retransmit at random times so that further collisions are reduced or avoided.

Collisions reduce the capacity of Ethernet below the 10-Mbps data rate. One of the unfortunate characteristics of Ethernet is that as traffic increases the collisions also increase. This is the reason for segmenting LANs, keeping the number of stations on a segment low and the cumulative offered load to below about 3.5 Mbps. The maximum frame size is 1500 bits.

Higher speed Ethernets at rates of 100 Mbps (Fast Ethernet) are available and deployable. Fast Ethernet running over UTP is referred to as 100 Base T. Many vendors offer NICs operating at either 10 or 100 Mbps to ease transition to the higher speed. Switches permit a mix of 100 Mbps and 10 Mbps ports and are provided with a mechanism to automatically detect the rate of an inserted card.

As a rule, increasing the data rate by a factor of 10 also reduces the operating cable length by a factor of ten. Therefore the higher speed Ethernets will operate over correspondingly shorter ranges. The protocol employed by Fast Ethernet is based on the original Ethernet; however timing characteristics are also scaled down by a factor of 10. Table 2 lists the Fast Ethernet family of standards. Fast Ethernet employs star configurations with point-to-point connections between LAN components. This is a key point when considering commonality of components. Fast Ethernet is not supported by coaxial cable.

Even higher speed Ethernets at gigabit-per-second data rates are being developed where a gigabit is 1000 Mbps or 1 billion bits per second. This network would operate at 10 times the rate of Fast Ethernet. Gigabit Ethernet is expected to become an IEEE standard by mid 1998, with products following within a few months.

**Table 2. IEEE 802.3/Fast Ethernet Family of Standards.**

| **STANDARD NUMBER** | IEEE 802.3u | IEEE 802,3u |
|---|---|---|
| **IEEE NAME** | 100 Base T | 100 Base FX |
| **MEDIA TYPE** | Unshielded Twisted Pair | Fiber |
| **OTHER NAME** | Fast Ethernet | Fast Ethernet, Fiber |

**When UTP cabling is employed as the interconnection medium, the NIC is provided with an RJ-45 jack. CAT-5 cabling is often employed between the computer and the hub.** CAT-5 cable consists of eight wires (four Twisted Pairs). Two pairs are used, one each for transmitting and receiving data. An RJ-45 plug is used on each end of the cable. One end of the cable plugs into the jack on the computer and the other end plugs into the wall jack or hub, if it is located in the same area. The maximum length of cable between any two devices, including patch cable and behind the wall wiring is 100 meters. This applies to both Ethernet at 10 Mbps and Fast Ethernet at 100 Mbps.

In the case where a wall is encountered, an RJ-45 Jack should be provided in the vicinity of the computer. The interconnecting cable would then plug into this jack (wall outlet). Internal building wiring would then route the jack to the hub.

**Installation of building wiring should be in accordance with EIA 568, the Commercial Building Telecommunication Wiring Standard, which defines a generic telecommunication**

**wiring system for commercial buildings that will support a multi-product, multi-vendor environment. It also provides direction for the design of telecommunications products for commercial enterprises. This standard establishes performance and technical criteria for various wiring system configurations for interfacing and connecting their respective elements.**

**In addition to the EIA/TIA 568 Standard, other useful documents available from EIA/TIA are:**

- **"Technical Service Bulletin-36," which defines additional cable specifications for UTP.**
- **"Technical Service Bulletin-40," which provides additional transmission specifications.**
- **"Technical Service Bulletin-53," which describes extended specifications for Shielded Twisted Pair Cables.**
- **"EIA/TIA 569," which describes the Commercial Building Standard for telecommunication pathways and spaces.**
- **"EIA/TIA 606," which describes standards for telecommunication infrastructure of commercial buildings.**

**Installation guidance is also available from a number of sources. One good site is on the Internet at:**

**http://www.dfrontiers.com:80/bicsi/tech/techsum/index.htm**

**When working with the cable, be particularly careful to:**

- **Avoid sharp corners,**
- **Avoid kinks or twists,**
- **Do not pull the cable with a force that exceeds the specified tensile strength. For indoor cable with no metallic strength members a safe limit is a maximum of 25 pounds of force.**
- **Keep it away from heat and moisture.**

**The bend radius of the cable should not be less than four times the outside diameter of the cable. The cable should be supported every 4 to 5 feet.**

## 3.3 WHAT DO I NEED?

**First, determine the number of users and their relative locations.**

In the discussion that follows, the word "user" is used in two ways. First, it is used to mean the person using the computer or, more specifically, the application on the computer or workstation. Second, it is used to mean the computer or workstation, or other device, physically attached to the network. In this second usage, the computer or workstation is acting on behalf of the person using it to perform the functions required by the person as it initiates, and responds to, activities on the network. The context in which the word is used should distinguish which use of the word is intended. In the current context, user refers to the device itself.

To determine the number of computers that will be connected to the LAN, as well as the network configuration, and the types of cable and quantity in linear feet to procure, a number of questions must be answered. It is necessary to know where to put the computers and how to interconnect the cables. This in turn will allow the determination of the supporting LAN components. Refer to Appendix C for additional questions.

Each question in the following discussion is given a number for reference, as the information provided will be used elsewhere in the process. The objective is to construct a set of worksheets or tables to characterize the network and cost out the components.

### 3.3.1 Computers and Applications

**To establish user requirements, an assessment of the needs of the organization personnel must be made. Information Technology (IT) is considered one of the key, if not the prime, enablers of Business Process Re-engineering (BPR). IT is the most powerful tool for reducing the costs of coordination. This will be achieved to the extent that collaboration is established. Collaboration, or functional coupling, of a process is the extent of information and mutual adjustment among participating functions. Innovative uses of IT will enable the coordination of activities that were not possible before, eventually raising the organization's capabilities and responsiveness. These potential benefits should be kept in mind while going through the process of requirements determination.**

To determine computer requirements, the following questions must be answered:

**Q 1. Does each person in the organization require a desktop computer?**

**Q 2. How many desktop computers will be required?**

- **a) Itemize by building.**

**Q 3. How many new desktop computers will be procured?**

- **a) Itemize these.**
- **b) Determine cost for these items.**

**Q 4. How many NICs will be required?**

**Q 5. What application software must be procured for each user?**

- **a) E-mail?**
- **b) Web Browser?**
- **c) File Transfer?**

**Q 6. What supporting application hardware must be procured?**

- **a) Mail server?**
- **b) DNS host?**
- **c) File server?**

### 3.3.2 Cabling

This section is provided for background information. It is recommended that contractor support be used to determine cable requirements and to install cables.

To establish the cabling requirements, inspection of building plans and actual physical measurements may be required. The network must be overlaid on the building plans. Start with locating the desktop computers and physically locate all infrastructure components.

It is generally not possible to run cables in a direct point-to-point manner from point A to point B within a building. Due to constraints within the building, a circuitous path must normally be taken in routing cables. Cables must be routed with regard to internal structures such as walls and wall outlets. For example, in a case where the general direction that cables should be routed is north, some cables might be routed in other directions, even south, due to the closest located wall outlet. This will increase the linear feet of cable needed.

If the impact of these constraints cannot be accurately determined, a “safety factor” will have to be applied. Where possible, especially with behind-the-wall wiring, it is good practice to run extra cabling to allow for expansion to accommodate additional users.

To determine the cabling required for the network, the following questions must be answered:

**Q 7. How would these computers be spread out in the area that the organization occupies?**

**a) Within a single building?**

**b) Within more than one building? How many?**

**c) What is the physical distance between each pair of buildings?**

**d) Do conduits exist for routing between buildings?**

**Q 8. What is the relative distribution of users within each building?**

**a) Clustered?**

**b) Distributed?**

**c) Both?**

**d) Estimate of linear feet of media required.**

**Q 9. Wall jacks and plates?**

**a) Locations relative to computers served?**

**b) Locations relative to wiring closets?**

### 3.3.3 LAN Infrastructure Components

To determine the infrastructure components required for the network, the following questions must be answered:

**Q10. What supporting hardware will be required?**

- **a) Switches**
  - **1) Port capacity**
- **b) Routers**
  - **1) External**
  - **2) Internal**
- **c) Hubs**

### 3.3.4 Cabling and Infrastructure

The questions given in Sections 3.2.1 through 3.2.3 are summarized in Table 3.

Questions 7 through 10 are directed toward the development of the network configuration by leading the reader through a process for determining how to lay out the equipment connectivity. This will most likely require several iterations before a "satisfactory" configuration is obtained.

Intra-building cabling can be summarized by floor level with inter-floor cabling added to that total.

Inter-building cabling can be routed in more than one way. Buildings can be cascaded or interconnected in a star configuration with one building as the distribution center. In either case, this cabling should be summarized on a per building pair basis.

**Once this configuration is determined, including the location of infrastructure components, the quantity of infrastructure components and the cabling to connect these components and the desktop computers can be estimated. The objective is to determine:**

**Inside Building Cabling**

- **Locations of RJ-45 wall plugs and plates**
- **Wall plugs to wiring closet cabling (behind the wall wiring)**
- **Inter-wiring closet cabling**
- **Desktop computers to wall plugs**
- **Inter-floor cabling (if not already included).**

**Inter-Building Cabling**

- **Length of cabling between building pairs.**

**Table 3. Summary of Questions.**

| |
|---|
| **Q 1. Does each person in the organization require a desktop computer?** |
| **Q 2. How many desktop computers will be required?**<br>a) Itemize by building. |
| **Q 3. How many new desktop computers will be procured?**<br>a) Itemize these.<br>b) Determine cost for these items. |
| **Q 4. How many NICs will be required?** |
| **Q 5. What application software must be procured? How many of each?**<br>a) E-mail?<br>b) Web Browser?<br>c) File Transfer? |
| **Q 6. What supporting application hardware must be procured? How many of each?**<br>a) Mail server?<br>b) DNS host?<br>c) File server? |
| **Q 7. How are these computers spread out in the area that the organization occupies?**<br>a) Within a single building?<br>b) Within more than one building? How many?<br>c) What is the physical distance between each pair of buildings?<br>d) Do conduits exist for routing between buildings? |
| **Q 8. What is the relative distribution of users within each building?**<br>a) Clustered?<br>b) Distributed?<br>c) Both?<br>d) Estimate of linear feet of media required. |
| **Q 9. Wall jacks and plates?**<br>a) Locations relative to computers?<br>b) Locations relative to wiring closets? |
| **Q 10. What supporting hardware will be required?**<br>a) Switches<br>1) Port capacity<br>b) Routers<br>1) External<br>2) Internal<br>c) Hubs |

### 3.3.5 Network Management

Protocols are available that support network management. Simple Network Management Protocol (SNMP) is the most commonly used. SNMP provides the capability for devices connected to the network to be managed, i.e., monitored and controlled. Management information is exchanged between devices and a management entity. **SNMP is defined in RFC 1157.**

Performance, configuration, and fault management capabilities are provided. SNMP provides a mechanism to baseline system operation and performance. Any change from the baseline can be determined. Faults or failures in system components can be located and isolated from the network.

The communication protocols, TCP/IP, are implemented with a software agent that locally monitors the operation of the station’s components and reports the activity to a designated manager. This operation is normally via a request/response information exchange initiated by the manager. However, should a situation arise whereby an event causes an out-of-tolerance condition, e.g., event counter exceeding a pre-established threshold, the agent will report this occurrence to the manager without waiting for a request by the manager.

## 3.4 SECURITY

It is critical to consider security aspects of the network. Security engineering guidance, like network planning guidance, is multi-faceted. Security engineering requires an understanding of the current technologies, the resolution of organizationally specific security concerns through engaging in a “questionnaire-type” process, and the establishment of a small reference library of supporting material. In addition, a clear understanding of the mission, the organization’s security policy, and the system/network configuration for a specific campus site is integral to the security architecture. Appendix A provides an overview of security, including risk analysis, as well as policies and mechanisms to mitigate these risks.

The Joint Technical Architecture and Technical Management Architecture Framework for Information Management (TAFIM), which contain multiple options and generic discussions, are useful starting points to provide an overall understanding of the environment and the security issues to be considered. To plan practical configurations, these overarching documents need to be complemented by detailed security considerations related to specific information protection mechanisms.

The “Defense Information Infrastructure Common Operating Environment (DII COE) Security Checklists,” which identifies specific NT security objectives associated with the DII COE NT configuration requirements is another useful reference. The rationale for each objective, operator actions to ensure proper configuration, and expected verification results are also included. Topics addressed include audit, access control, file system security, FTP, user identification and authentication, password management, network services, and system architecture. In addition, security objectives for UNIX, Data Base Management System (DBMS), and Distributed Computing Environment (DCE) capabilities are also provided.

This item and other documentation related to DII COE can be found at URL:

**http://spider.osfl.disa.mil/cm/cm_page.html**

The following two useful references should be available within your organization:

**“Department of the Navy Automatic Data Processing Security Program (OPNAVIST 5239.1A),” August 1982.** This instruction contains the DoN Automatic Data Processing (ADP) security manual containing information on policies, procedures, and responsibilities for establishing and maintaining ADP security programs at all levels within the DoN.

**“Department of the Navy Information Systems Security (INFOSEC) Program (SECNAVIST 5239.3),” 14 July 1995.** This instruction contains the DoN policy for the INFOSEC Program within the information warfare discipline and defines the organizational responsibilities for implementation of the security disciplines of COMSEC, COMPUSEC, and TEMPEST.

Prior to network implementation, it is necessary to assess security risks and develop security policies. Security must be engineered into the network from its inception. It must be an integral part of the process of design. It is difficult and expensive to add security to the network as an afterthought.

Two particular areas of concern are discussed below.

Inter-building cabling was discussed in section 3.2.4.2. The cable between buildings presents a point of vulnerability from a security perspective. Unless all the buildings are within a protected perimeter, consideration should be given to intrusion detection. Typically, this conduit would be buried underground. The cable within the conduit may have to be of a special type in military installations, in addition to being physically protected.

Another security point of vulnerability is the external/internal network boundary. Official information internal to the organization or information that should not be disclosed to the general public must be protected. Firewalls can be implemented on routers. Conceptually, the firewall places a control or protection layer between your network and the rest of the world. This layer permits some traffic through while prohibiting other traffic. The router screens traffic based on criteria such as the IP address of arriving or departing traffic. Thus, a firewall should be placed between the switch and the point where the Internet connection makes its appearance. This is illustrated in Figure 7. Physical access to this router should be restricted**.**

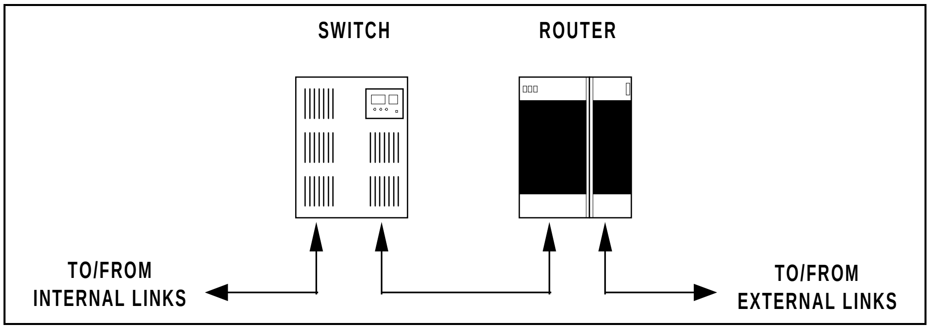


**Figure 7. Internal/External Link Connectivity.**

**It is suggested that these specific recommendations be followed:**

**Understand the threats to the system.** In addition to Internet access via TCP, take into consideration access control requirements such as the sensitivity of the data, the range of security clearances for internal users, each individual user's access to sensitive data, need-to-know access, access to/from other LANs, dial-up capability for authorized users, and access to the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) or the Secret Internet Protocol Router Network (SIPRNET).

**Address the need for a network security policy and provide a set of guidelines to facilitate consistency among installations.**

**<u>Example:</u> Systems requiring access controls include:**

- Systems processing classified or sensitive data.
- Mission-critical systems.
- Systems with connections to external networks.
- Systems with inbound modem pools.
- Systems with Web servers.

**Assess the security posture of specific host configurations (including different security features of applicable operating systems and mission-critical applications), and apply protection capabilities to enhance that posture (see DII COE Security Checklists).**

**<u>Example:</u> A limited set of security configuration guidelines for a server might include the following generic concepts.**

- Minimize operating system configuration by disabling risky services such as Trivial FTP.
- Disable IP forwarding and source routing.
- Avoid dual-homed server configuration.
- Implement current operating system and security patches.

- Ensure server operates with fewest privileges possible.
- Limit implementation of additional servers on same machine such as FTP and mail servers.
- Limit functionality on server and restrict types of operations.
- Detect unauthorized changes to machine configuration.
- Monitor server logs, and keep abreast of incidents and advisories.

**Example:** **A limited set of security configuration guidelines for a router might include the following generic concepts.**

- Disable Address Resolution Protocol (ARP) and route processing, defaulting to static tables.
- Install an ARP entry for the external and internal hosts.
- Set up an initial packet filter that denies access to all hosts, and then permit access to inside and outside hosts.

**Example:** **A specific implementation for setting up anonymous FTP with the standard UNIX FTP server is described in "Practical UNIX and Internet Security," 2nd Edition, O'Reilly and Associates, pp. 491-493.**

**Example:** **A specific implementation for setting up DNS is described in "Building Internet Firewalls," O'Reilly and Associates, pp. 278-296.**

Assess the need for network security components including firewalls, mail guards, intrusion detection capabilities, encryption, network security tools, and communications servers; and manage/maintain those components to ensure continuous protection.

**Example:** **A firewall is recommended for systems that:**

- Connect to external networks.
- Consist of a large number of hosts.
- Service a large number of users.
- Support mission-critical functions.

**Contact SPAWAR PMW 161 for further information on INFOSEC. Also, see references OPNAVIST 5239.1A and SECNAVIST 5239.3.**

## 3.5 PROCESS FLOW, OR, PUTTING IT ALL TOGETHER

### 3.5.1 The Network Plan

Effective networking starts with effective planning. In essence, the network should be planned carefully before any funds are spent. This section provides a road map that will be amplified in Appendix C. Table 4 provides an overview of the process.

**Table 4. Developing the Network Plan.**

| | |
|---|---|
| 1. User Expectations. | Express anticipated needs in terms both specific and vague; solicit input from all involved, uninhibited by “practical considerations” but tempered with “good sense”; consider both current and future needs. |
| 2. Functional Requirements. | Order and prioritize needs and then establish a realizable, complete, and consistent set of requirements derived from those needs. |
| 3. Resource and Operating Conditions Assessment. | Make a preliminary accounting of what resources are available with respect to funds, plant assets, capital equipment, and in-house expertise and skills; determine expected operating conditions (such as where equipment and cable might be located, etc.); determine factors bearing on installation – such as regulations (building codes, security, etc.), power availability, number of potential users and their location, preexisting future planning, etc. |
| 4. Design. | Use an iterative process that proceeds through finer degrees of detail at each pass to establish a specific design that balances all the factors (available resources, design requirements, regulations, etc.) to satisfy the requirements to the “best” degree possible; observe requirement priorities, accomplishing the most important immediately and planning for incorporation of other requirements in the future; consider (ease of use), reliability and maintainability (and maintenance cost), availability, etc. |
| 5. Definition. | Identify all the equipment required, labor to be performed, accommodations that need to be made in the existing plant to receive the installation, and additional equipment, training, etc., that may be required by the “users” to benefit from the installation; revise the cost estimate as necessary and verify funding; determine steps to accomplish installation. |
| 6. Acquisition. | Order equipment; arrange for labor; prepare plant to receive installation. |
| 7. Installation and Setup. | Install cable and equipment; set up and establish operation. |

**(Table 4 continued on next page.)**

**Table 4. (Continued)**

| | |
|---|---|
| 8. Evaluation. | Verify (transport) operation as planned. |
| 9. Application. | Introduce new capabilities to users; establish auxiliary network operations; establish operations and maintenance functions. |
| 10. Operation. | Deal with day-to-day operation; routine maintenance, repair. |
| 11. Training. | Train personnel to deal with various aspects of network operation, maintenance, and upgrade. Train users on the utilization of network applications. |

Appendix C is organized into a series of user fill-out forms and narratives that can be blended into a network plan. Terms and definitions in the table describe each particular step. The forms in appendix C can be reproduced and placed in a 3-ring binder for use in network planning. Planning should not be rushed, and the network should not be implemented until all planning steps are complete. The most costly mistakes are the ones made before installation begins.

### 3.5.2 A Scenario Example

Appendix D provides a scenario example, demonstrating the process via filling out the forms presented in appendix C for a specific case. The scenario used is the following:

1. Flag Aide for a 30-person staff.
2. Admiral wants electronic mail.
3. Additionally, they want two new network printers (1 color, 1 B&W).
4. All staff work in a single building.
5. They have heard about DMS and want to plan for the future.
6. Their complement of computers consists of the following:

   a. Equipment: 1 Macintosh System 7

   b. 5 Pentium Windows 95

   c. 1 80286 MS-DOS 6.22

   d. 1 80386 Windows 3.11

   e. 7 80486 Windows for Workgroups 3.11

   f. No UNIX-based components

## 3.6 COST DETERMINATION

### 3.6.1 Components

Considering the answers provided to the questions posed in Sections 3.2 through 3.4, Table 5 can be constructed to calculate the estimated component costs. This table is an example. Several items, e.g., "Computers," may require more than one row depending on how many brands, models, and options are being procured. Also, Items 9 and 10 could require extension if several buildings are involved.

**Table 5. Cost Tabulation.**

| ITEM | NOMENCLATURE | QUANTITY | COST PER ITEM | TOTAL COST |
|---|---|---|---|---|
| 1. Computers | | | | |
| 2. NICs | | | | |
| 3. E-mail Software | | | | |
| 4. Web Browser | | | | |
| 5. File Transfer | | | | |
| 6. Mail Server | | | | |
| 7. File Server | | | | |
| 8. DNS Host | | | | |
| 9. Building Cable/Building:<br>a. Wall Plate to Wiring Closet<br>b. Computer to Wall Plate<br>c. Floor to Floor | | | | |
| 10. Building to Building Cabling | | | | |
| 11. Switches | | | | |
| 12. Routers<br>a. External<br>b. Internal | | | | |
| 13 Hubs | | | | |
| **TOTAL COST** | | | | |

### 3.6.2 Installation

A choice, if it applies to your situation, of installation personnel must be determined. Is in-house expertise available? If not, is a local contract vehicle available at your facility for this kind of service? If not, see Section 4.2 for information on possible sources of assistance. Costs will depend on the personnel resources used for hardware and cable installation.

## 3.7 CONNECTIVITY BEYOND THE LAN

While this guidebook specifically addresses connectivity on the LAN level, for illustrative purposes examples of Campus Area Network (CAN) connectivity will be briefly described in this section. For connectivity beyond the immediate organization level, it is advisable to check with Base Communication and/or Civil Engineering personnel.

The base may have a situation where buildings are separated by more than the 0.5-mile radius of the LAN. Figures 8 and 9 show interconnectivity of clusters of buildings where the clusters are beyond the LAN limit. A LAN is shown within each building cluster. Each box within the larger box represents a building. Due to resolution limitations, only the connectivity between the buildings in the cluster is presented. Each building might have its own switch for connecting the building computers, servers, and network equipment. The buildings within the cluster are interconnected via Ethernet technology. Ethernet or Fast Ethernet may be used as requirements dictate. The interconnection of building clusters employs different technology.One building within each cluster is equipped with a switch with ports providing the appropriate Ethernet technology for the buildings of the cluster. The switch also has a port providing the interface to the backbone.

Figure 8 shows how Asynchronous Transfer Mode (ATM) may be employed to achieve this connectivity. ATM is an emerging switch-based technology that is still undergoing standardization. It supports several rates of transmission, with the current common rate of 150 Mbps. It is a circuit-based technology analogous to the public telephone system. A fully connected network can be configured by connecting the switch in building cluster 1 to the switch in building cluster 4, and the switch in building cluster 2 to the switch in building cluster 3.

Figure 9 shows how Fiber Distributed Data Interface (FDDI) might be used. FDDI uses a ring topology. FDDI uses the more orderly Media Access Control protocol of token passing, so it does not suffer the collision drawback that Ethernet encounters. The transmission rate is 100 Mbps. In each case, the Service Delivery Point for MAN/WAN connectivity is shown.

Since the subject of this document is LANs, the relative merits of ATM and FDDI will not be discussed. References are available where further information may be obtained. Textbooks are available at local libraries or technical bookstores. Sources are also available on the Internet.

For ATM information, point to:

**http://cell-relay.indiana.edu** This site provides links to additional sites.

For FDDI information, point to:

**http://sholeh.nswc.navy.mil/x3t12/fddifaq**

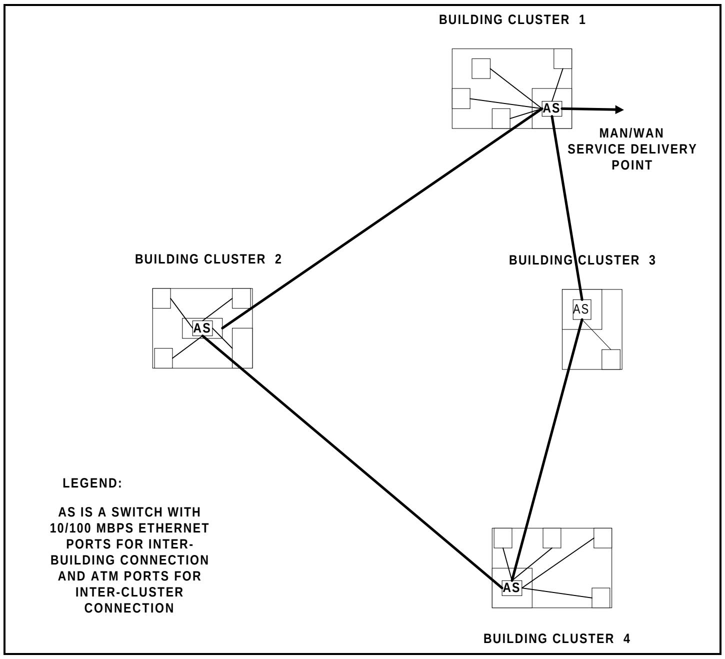

BUILDING CLUSTER 1
AS
MAN/WAN SERVICE DELIVERY POINT
BUILDING CLUSTER 2
AS
BUILDING CLUSTER 3
AS
LEGEND:
AS IS A SWITCH WITH 10/100 MBPS ETHERNET PORTS FOR INTER-BUILDING CONNECTION AND ATM PORTS FOR INTER-CLUSTER CONNECTION
AS
BUILDING CLUSTER 4

**Figure 8. Using ATM for Campus Connectivity.**

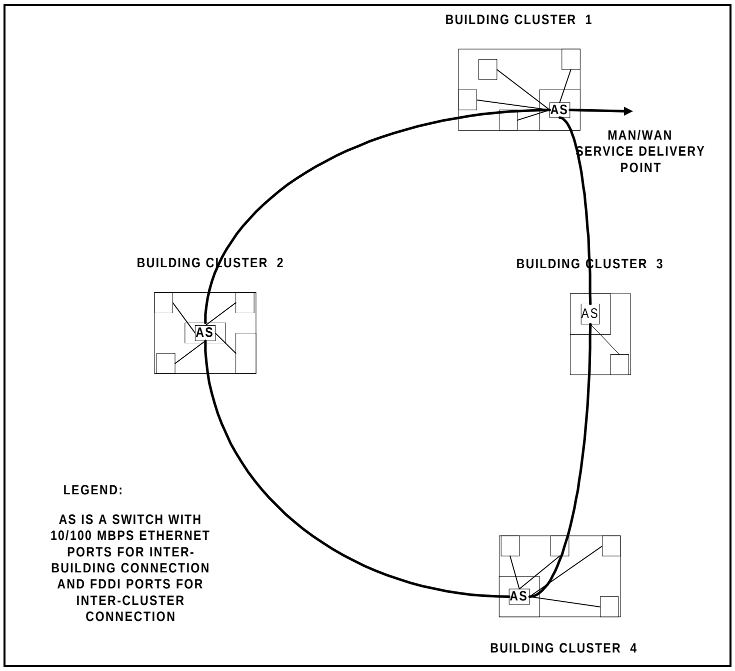

BUILDING CLUSTER 1
AS
MAN/WAN SERVICE DELIVERY POINT
BUILDING CLUSTER 2
AS
BUILDING CLUSTER 3
AS
LEGEND:
AS IS A SWITCH WITH 10/100 MBPS ETHERNET PORTS FOR INTER-BUILDING CONNECTION AND FDDI PORTS FOR INTER-CLUSTER CONNECTION
AS
BUILDING CLUSTER 4

**Figure 9. Using FDDI for Campus Connectivity.**

# 4. PROCESS FOR ACCESS TO SYSTEM ENGINEERING ASSISTANCE

## 4.1 DoN CHIEF INFORMATION OFFICER (CIO)

The Department of Navy Chief Information Officer (DoN CIO) provides leadership, guidance, and support to the DoN Information Management/Information Technology (IM/IT) community and ensures the implementation of IM practices that support the goals and objectives of the Navy and Marine Corps. The DoN CIO was established primarily as the result of Congressional IT legislation, the Clinger–Cohen Act of 1996. The Office of DoN CIO was formally instituted in June 1997 by the direction of the Secretary of the Navy. DoN CIO’s primary near-term objective is to establish enterprise-wide IM/IT policies for the Navy and Marine Corps, particularly in the areas of architectures, standards, and security. Organizations are strongly urged to contact the Office of DoN CIO for facilitation of system engineering or for other assistance with their IM/IT efforts. Specifically, contact should be made if networking will be established to the Navy at large in order to assure interoperability within the Navy and compliance with Navy IM/IT policies. For further information, visit the DoN CIO website at www.doncio.navy.mil or contact brightfuture@hq.navy.mil or call (703) 602-2104.

## 4.2 OTHER SOURCES FOR ASSISTANCE

A number of Government Umbrella Contracts are available. These umbrella contracts are designed to satisfy the needs of government users having the same general requirements for information technology: hardware, software, data communication, and support services.

The URL to access this information is:

**http://www.chips.navy.mil/it/index.html**

The site was established to reduce overall costs and expedite the processing time involved in the acquisition of information technology resources. This site provides links to the actual contract information.

The site also includes links to the newly awarded Voice, Video and Data (VIVID) contracts.

# 5. REFERENCES AND RESOURCES

## 5.1 DOCUMENTS

This guidebook will be maintained to provide information as current as possible. The reader is cautioned to check these references and use the latest version available.

- **"Technical Architecture Framework for Information Management (TAFIM)," Volume 3, March 1997.**

  **Point of Contact: William Wong (703)-735-3228**

- **"Joint Technical Architecture (JTA)," Version 1.0, August 1996.**

  **Point of Contact: Wil Berrios (703)-735-3552**

- **"The Defense Information Infrastructure Common Operating Environment (DII COE) Documentation and Security Checklists"**

  **Point of Contact: Hotline (703)-735-8681**

- "Navy Base Level Information Infrastructure (BLII) Master Plan 1996-2007," Version 2.0, June 1996.
- "Department of the Navy Automatic Data Processing Security Program (OPNAVIST 5239.1A)," August 1982
- "Department of the Navy Information Systems Security (INFOSEC) Program (SECNAVIST 5239.3)," 14 July 1995
- **"Networking for Dummies," Second Edition, 1996. Published by IDG Books Worldwide, Inc. Foster City, CA.**
- **"Practical UNIX and Internet Security" 2nd Edition, O'Reilly and Associates, pgs. 491-493.**
- **"Building Internet Firewalls," O'Reilly and Associates, pgs. 278-296.**
- **"Network Computing" Magazine**

  **Applications for subscriptions should be addressed to Network Computing, 600 Community Drive, Manhasset, NY 11030. Telephone 847-647-6834. FAX 847-647-6838. Other correspondence: telephone 516-562-5071; FAX 516-562-7293.**

- "LAN Tutorial," Editors of LAN Magazine; ISBN 0-87930-379-4.
- **IEEE**

  **Applications for copies should be addressed to the Institute of Electrical and Electronic Engineers, 445 Hoes Lane, Piscataway, NJ 08554-4150.**

- **EIA/TIA**

  **Applications for copies should be addressed to Global Engineering Documents, 15 Inverness Way, Englewood, Colorado 80112 5704.**

- **IETF RFCs**

  **Applications for copies of RFCs should be addressed to Network Information System Center, SRI International, 333 Ravenswood Ave. Room EJ291, Menlo Park, CA 94025.**

## 5.2 WEB SITES

- **TAFIM:**

  **http://www.library.itsi.disa.mil/tafim/**

- **JTA:**

  **http://www.jta.itsi.disa.mil/jta/**

- **DII COE:**

  **http://spider.osfl.disa.mil/cm/cm_page.html**

- **DMS:**

  **http://www.disa.mil/D2/dms/docs/progovw/toc110.htm**

  **and**

  **http://www.spawar.navy.mil/~DMS/index.html**

- **IT-21:**

  **http://www.inpo.navy.mil/it-21/index.html**

- **ITEC Contract:**

  **http://www.part.net/itec/itec.html**

- **IETF RFCs:**

  **http://ds.internic.net/ds/rfc-index.html**

  **or**

  **http://info.internet.isi.edu/1/in-notes/rfc**

**Note that depending on their individual status, RFCs might be replaced or deleted. If replaced, this will be annotated in the index with a pointer to the later RFC.**

- **Internet Internic:**

  **http://www.internic.net/**

- **EIA 568, Building Wiring Installation:**

  **http://www.dfrontiers.com:80/bicsi/tech/techsum/index.htm**

- **Network Computing magazine Web Site:**

  **http://techweb.cmp.com/nc/netdesign/series.htm**

## 5.3 RESOURCES

**Internet Addresses and Domain Names:**

**The Navy Domain Name Service (navy.mil and navy.smil) has transitioned to Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMSLAN).**

**For NIPRNET, all DNS request/inquiries should be sent to**

**hostmaster@uar.navy.mil**

**For SIPRNET, all DNS request/inquiries should be sent to**

**hostmaster@dnsmail.uar.navy.smil.mil**

# APPENDIX A: SECURITY

## A.1 INTRODUCTION

Making your network more secure requires a little time and a good understanding of what the risks are and how you can avoid or negate them. The difficult part of security is understanding, and getting your users to understand, what the risks are and what operating procedures must be followed to maintain security. Information security is not static. It will require a significant investment of time to remain abreast of the current issues. This appendix will give you enough basic information and pointers to new information necessary for building a more secure network.

This appendix is organized into four sections. First, it is extremely important to dispel some of the myths surrounding information security (and to provide you with information to allow you to "speak the language" of security). The risks are covered in great detail in the second section. The third and fourth sections are the meat of this appendix, covering the practicalities of securing the user, and the network. If your time is limited, you might jump ahead to these last two sections. At the end of the document, a bibliography and pointers to many different resources will help you find more information on both specific and general topics on information security available on the World Wide Web and at your local bookstore.

## A.2 SECURITY MYTHS AND LEGENDS

First, lets dispel a few myths. These myths tend to be perpetuated by the media, people unfamiliar with computers, and people who just do not know any better.

***Myth #1****: There are some really good operating systems, such as Windows NT or HP-Secure OS CMW, that make the system completely secure.*

First of all, there is no truly secure system, much less a truly secure network. There are too many variables in the life of a system or a network that just cannot be controlled. The best you can do is to make sure that you have done everything to make sure that the system is as secure as possible, so that you can detect an intruder and deal with him appropriately before he gains access. Windows NT and HP-Secure OS, as well as every other operating system on the market have bugs (flaws) that can be exploited by a hacker. Software manufacturers release bug patches and software service packs that allow the Administrator to fix these bugs. Taking the time to install these fixes will bring you one step closer to a secure system.

***Myth #2****: Most systems are attacked from the outside.*

According to a recent study of companies breached by hackers, 80% of the systems attacked were attacked by insiders, either people wanting to expand their capabilities beyond what a system administrator had designated for them or by disgruntled employees.

***Myth #3****: Computer hackers are usually pre-pubescent teens or immature adults who do not have very many friends or social relationships, who hack into systems on a crusade for environmental or other causes.*

Actually, quite the opposite is true. Since 80% of the systems attacked were attacked by insiders, most of the hackers are people you probably would hire. Hackers are quite social, and usually form groups of hackers, known as a hacker communities. These communities tend to operate for as long as it is required to achieve a specific task, then break up.

***Myth #4****: Our computers do not have anything on them worth protecting; therefore we do not need security.*

Wrong! Security through obscurity is not security. The fact that your computer is on the network makes you vulnerable to attack. If you are on a .mil domain, you are even more vulnerable because an attacker who has access to your machine can get access to much more sensitive data than those who are on other domains. Most military and government institutions offer “intranet” access to those users who access their site via a .mil domain. Gaining access to a machine that exists within the .mil domain makes it easier for an attacker to gain access to these intranets, where they do not belong.

## A.3 THE RISKS

The best method of defense is understanding where the attack will come from. If you do not fully understand the risks, you cannot prepare to handle those risks, and you become ineffective. Though some of these risks (most notably the virus infection risk) are not commonly used by hackers to gain access to your network, they are notable risks.This is illustrated in Figure A1.

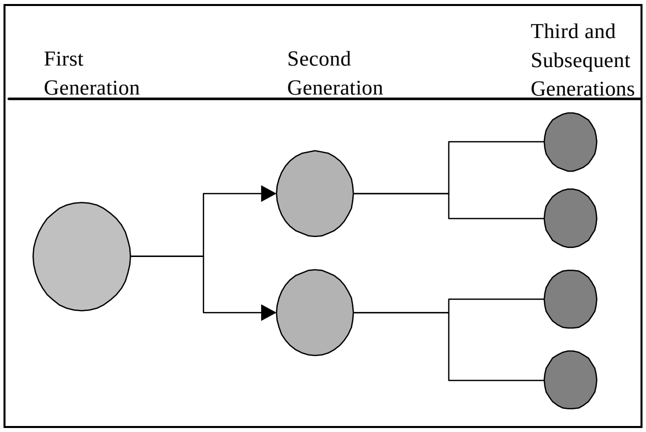


**Figure A1. Virus Infections.**

## A3.1 Virus Infections, Trojan Horses, Internet Worms

A virus infection is the most abundant risk on the Internet, where files and documents are transferred from one machine to another with the very little effort involved. Computer viri (plural for virus) are pieces of self-reproducing malicious code appended to a document or executable program that when executed or viewed, cause data to be damaged or destroyed, either by intent or otherwise. Viri always reproduce by infecting other executables or documents on the computer. Most viri spread by copying themselves into memory, and then into any executable that is run while the virus is in memory. Some viri do not need to copy themselves into memory, but reproduce by copying themselves into every executable they find in the drive or directory in which they are running. The most abundantly found viri on the Internet are the Word Concept viri, which attach themselves to Microsoft® Word documents, and are spread via infected Microsoft Word programs. This derivative of a virus spreads faster than its older counterpart (the executable virus), mostly because the proliferation of the use of Word documents as attachments to E-mail.

Virus infections can be used by hackers to gain access to your network, though it is not as common as some of the other methods of attacks. A virus can be planted by a hacker into a file that you download or use. When the virus is run, it spreads itself into all of your executables. If the virus finds an executable responsible for auditing or security, it can delete that program. Then, at a predetermined time, the virus can pop-up a dialog box on the screen asking you to re-enter your password. This password can then be sent back to the hacker without your knowledge, allowing them to log into your computer.

Trojan Horses are much like viri, but they cannot reproduce themselves. Instead, Trojans rely on the user to run them before they can do their work. Trojans usually are touted as having some useful purpose. A notable Trojan Horse is the AOL4FREE Trojan, which when run, is supposed to allow a user to gain access to America Online for free. Its main purpose, however, is to destroy the user’s hard drive, which it does promptly after it is run. Trojans are also used by hackers much more frequently than viri. Usually, after a hacker has gained access to a system, he uploads several Trojan programs to the system that he can use as backdoors and password sniffers if the system administrator shuts down his primary access to the system. A common Trojan used by hackers is the login Trojan. This Trojan takes the place of the normal UNIX login program, which takes care of the user login functions of the UNIX operating system. The Trojan sends a copy of the login information it receives from the user and sends it off to the hacker. This login Trojan also has a backdoor, allowing the hacker to gain system administrator access to the machine in the case that the system administrator has locked the hacker out. Novell and Windows NT machines are also prone to these types of programs.

Internet worms are self-replicating programs that operate on the Internet instead of on your PC. They operate by replicating themselves across machines, jumping from one machine to the next. Some Internet worms serve a useful purpose, like web-bots, which jump back and forth from web page to web page, sending the information it obtains back to a search engine such as Yahoo or Alta-Vista. Other Internet worms are used by hackers to obtain information about the topology of a section of the network that they wish to attack.

The insideous natures of viri and worms are depicted in Figure A2.

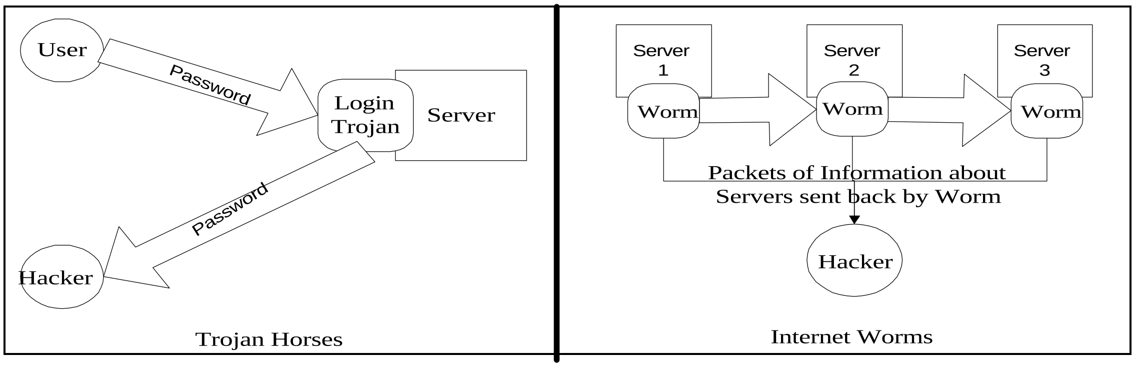


**Figure A2. Trojan Horse and Internet Worm Attacks.**

Internet worms can also be used to create a denial of service (see next topic) by causing a server to be overloaded.

### A.3.2 Denial of Service

Denial-of-service attacks usually do not disclose or destroy data on a server, but they will make your server unavailable to your users. This can cause more damage than the loss or disclosure of sensitive data because your legitimate users will be unable to get access to that data while the server is off-line. “Ping O’Death” and “Out-of-Bandwith” denial-of-service attacks are among the more well-known attacks, though both are now easy to correct through software bug fixes. Unfortunately, denial-of-service attacks are much easier to perform than the other attacks against your machines. Denial-of-service attacks may also be used as a method of gaining access to a system as well.

If your network security tools are not set up correctly, hackers can disable them and therefore gain access to the machine they wish to attack without being detected. For instance, if a firewall is set up to allow all traffic to continue after it is shut down, a denial-of-service attack on that system could potentially allow a hacker to subvert your firewall to gain access to your internal network.

Figure A3 shows a denial-of-service attack.

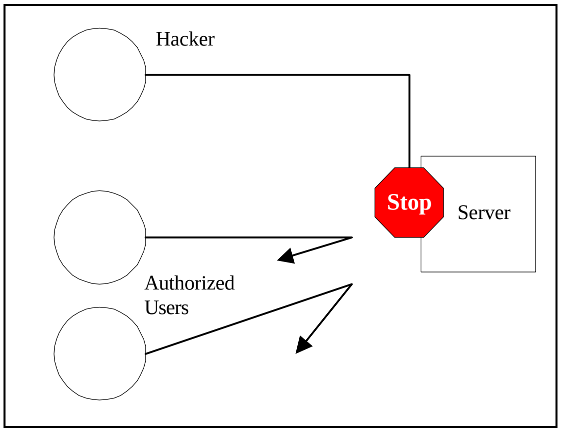


**Figure A3. Denial-of-Service Attack.**

### A.3.3 Disclosure of Information

Disclosure of information occurs when a hacker has gained access to sensitive data on a system, and then either sells that information or uses that information for personal gain. Under DoD guidelines, no classified information can be stored on a computer hooked up to a unsecured network. However, many of the machines within your network will probably be used for non-classified but sensitive data, such as contract, payroll, electronic correspondence, and proposals, that could cause serious problems if compromised. Disclosure of this information may result in criminal action and Congressional investigation.

Disclosure of information attacks can happen in several different ways. First, a server could be hacked into using an account with a lifted or weak password, and the data could be taken directly from the server. This is usually difficult to do, although an experienced hacker can use tricks such as attacking new accounts on a server or by looking for users who appear to know little about computers, and thus prey on their ignorance through weak password guessing or social engineering. Another method of disclosure of information is using a “man-in-the-middle” attack, which involves hijacking a connection between two trusted servers. An attack using this method is a little easier, and usually allows a hacker to use the hijacked connection to gain access to one or both of the machines.

Loss of anonymity is another danger that falls under the disclosure of information. When using a web browser or other client software package, you may be publishing information about yourself to the world. This usually results in very little disclosure of information, but the information can be used to track your movements throughout the network, or can be used to form mailing lists or other information.

Undesired disclosure of information is shown in Figure A4.

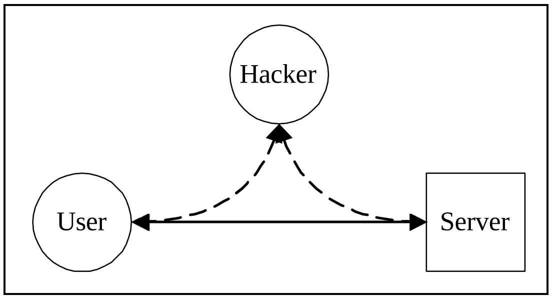


**Figure A4. Disclosure of Information Attacks.**

### A.3.4 Violation of the Integrity of Information

A violation of the integrity of information attack inserts viri into executable programs on a system, or scrambling or destroying data on the system. Recent examples are attacks in which Department of Justice and CIA pages were broken into and “edited.”

### A.3.5 Fraud

Fraud on the Internet is quite easy, since there is no easy way to know that the person you are communicating with is really who they say they are. Two methods of fraud can cause problems. The first is “spoofing,” or taking someone else’s identity as your own. The second is fabricating an identity, then using it as your own.

### A.3.6 Theft of Computing Resources

This is not as much of a risk as the others, but it could be a problem if your systems are used for real-time applications, or in situations where computing resources are limited. The hacker could use valuable system resources such as hard disk space or memory to store data that he is taking from other systems, or the hacker could use attached printers to waste paper. The system could also be used as a stepping stone for attacking other systems, or as a platform for network password sniffers or Trojan Horses.

## A.4 SECURING THE USER

There are two reasons for securing the user. First, the user is often the weak point for the whole system, giving passwords away to coworkers and giving security information away to strangers that call on the phone. Second, the user can also be the culprit.

### A.4.1 Secure Passwords

A weak password is a password that is easy to guess. Weak passwords usually are common keyboard combinations (“12345”), common phrases, common names, or anything found in the dictionary. User-specific information is also usually considered weak, especially if that information is something that could be found in a phone book or in public records. Social security numbers, drivers’ licenses, and mothers’ maiden names are usually bad choices for passwords.

Many users will choose ineffective passwords for the sake of remembering the password. This is mainly because the user is unaware of the dangers of weak passwords. A user would much rather choose a password that is easy for them to remember rather than suffer embarrassment or loss of capabilities for forgetting their passwords. Unfortunately, weak passwords are the first exploit a hacker will try, which means the user is actually helping the hacker out by choosing a weak password.

Require or persuade your users to choose secure passwords. Many programs, such as npasswd and crackpwd, reside on a UNIX machine and check the user’s password to see if it is in the dictionary. Windows NT 4.0 Service Pack 3 adds the ability to Windows NT to check for weak passwords, though there are much better third-party password checkers available for Windows NT, Windows 95, and Windows for Workgroups. These programs will require the user to choose a strong password instead of a weak password. You can also use a program that generates a listing of strong passwords, then allows the user to choose one of the passwords on the list.

Persuading a user to choose a strong password can be difficult, since users will resist choosing a hard-to-remember password, instead choosing a weak password that is easy to remember. Usually, if persuasion is used to choose a strong password, something is included in policy to state what a weak password is and how to avoid using weak passwords. Be careful on setting policy on password choices, since some users will follow policy literally instead of figuratively. Do not give users specific examples of strong passwords, since some users will choose to use the examples you give them as their password, a practice you are trying to avoid. Explain to the user that if someone breaks into their account, they are responsible for whatever damages occur. Doing so usually encourages the user to choose a good strong password.

### A.4.2 Removing Users after Severance

When dealing with networks or servers, a user who no longer works for an organization should be removed immediately. Under most circumstances, a user leaving a particular organization leaves under good circumstances, and leaving their account active on the server is usually harmless. However, it is a good security practice to remove the user from all access lists for all organization machines when they leave. Terminated user accounts must be removed from all the organization's computers. This keeps a user from gaining access to information they are no longer authorized to receive. It will also keep a former employee from using the organization's information for his/her personal or professional gain.

Sometimes, an employee leaves the organization under unfriendly circumstances, in which case, leaving their account open may prove to be dangerous. If the account remains active, a disgruntled employee can use their account to retaliate against the organization. Unfortunately, it is not uncommon for an employee who is terminated under unfriendly circumstances to retaliate against their employer.

To facilitate the removal of severed employees, many companies require that managers contact the system administrator about the loss of an employee before the employee leaves so that the account can be removed. Such a requirement should be written into the organization's policy.

### A.4.3 Computer Policy

There are many ways to secure the user, but the best method is to use a system-wide policy that is enforced strictly and evenly. There are many DoD-wide policies in place that can help steer you in the right direction, but it is best not to lean too heavily on the DoD-wide policies, since there are many cases where those policies are vague or impractical. The idea is to write effective policies that will stand up in a court of law while remaining fair to both the user and the organization. The DoN Automatic Data Processing (ADP) Security Manual and the DoN Information System Security Program Instruction, as well as the Orange Book (Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83, 15 August 1983), are all helpful resources for writing policy. There are also several good sites on the WWW that have written policy and security information; check the back of this appendix for these sites.

The problem with writing policy is that often policy gets too vague and difficult to enforce. Policies should be written in such a way that a user knows what they can and cannot do, while also allowing the user to create their own operating procedures. Users would much rather do the minimum number of tasks with the minimum expenditure of time and resources. Security procedures are going to be ignored if the user does not realize that security is important to them, as well as to you, your supervisor, and the U.S. Government. Writing policy that takes this into consideration will make policy more acceptable.

The security policy should be enforced evenly across the organization. Enforcing a security policy for employees while loosening up on the management is bad policy, and could get an organization into trouble when hackers target a management account that is poorly guarded. Management is notorious for handing out passwords to secretaries, yet they would get upset at a user giving their password to another user in the organization.

### A.4.4 Well-Written Policy vs Poorly Written Policy

Everyone wants their policies to be well written, easy to understand, and easy to follow, yet very few policies end up that way. This is partly because policy is usually written after-the-fact, or as an addendum to a problem that has occurred in order to keep it from happening again. Policy is often written quickly by one person, without giving much thought to the process other than to get it out to the users before anything else happens. This is not good practice, and should be avoided. Policy should be well thought out, well planned, and though one person can write effective policy, they should have others review it to make sure that their policy is efficient and effective. The policy should then be agreed on by the users (which gives the users the opportunity to “own” the policies that they will be expected to follow.)

Well-written policies are written in general terms, not specific terms. While specifics should be avoided, generalizations should not be too vague or impractical. Rules about passwords are often a great example of the difference between good policy versus bad policy. Stating, “Please take extra precautions to make sure that your password is protected from disclosure,” is much better than, “Don’t write your password down.” Very few people can actually remember a randomly generated password on the first try, so many will write it down, regardless of what the policy states. Worse yet, they may use easy-to-guess passwords instead, which is just as bad as writing a password down on paper. By telling users to guard their password carefully, they are much more apt to vigorously protect that piece of paper than those who break policy by using an easy to guess password.

Policies should state what you want a user to do or not to do with their computer. Policies dictating usage of organization time and resources are too specific to be effective. Policy statements such as “Users should not point their browsers to Playboy” are not very effective, because users will just point their browsers to other non-productive sites instead. A statement such as “Organization time and resources should be used for organization projects and business” is more effective, because it essentially sums up what you wish to accomplish (whether it be on the computer or around the water cooler) without being too vague.

## A.5 SECURING THE NETWORK

Many tools and techniques are required to secure the individual systems and networks. You will want to download the various tools available and use them. Most come with a very specific set of instructions, which you should print out and use.

### A.5.1 The New Security Model

In the days of the Wild West, banks stored money in vaults to protect it from being stolen. Guards were often employed to protect the vaults. But with little effort, robberies were often successful. And robbers could usually get away before a sheriff could respond. Banks often covered up the attacks, because they believed that a customer's confidence in the safety of their money was more important than the loss of the money. Safes were made more secure, but robbers again found ways to get into them. Gradually, the telegraph, telephone, and other advances allowed a faster response time from authorities.

Now, safes are rated according to the time it would take to break into the safe. Banks use this amount of time as a cutoff for the amount of time it would take to thwart a robbery attempt. Banks learned that they had to make the time to detect and then react to the robbery shorter than the time the protection could be maintained.

Computer security experts have always tried to secure their computer systems against hackers. After every attack, they would cover up the attack and fill any holes in the operating system. Rarely was any attack made public, lest management or customers lose confidence in the safety of the data on their systems. They would build bigger "vaults" around their computer systems, sever all ties with other networks and other machines, and eventually make the machine very difficult to use.

Now, computer security experts are gradually moving in the direction that banks were forced to move. Unlike banks, hackers could be as close as next door or as far away as Moscow, Russia, but still, making the time required to detect and react to a computer break-in shorter than the time the protection could be maintained seems to be the better route. You will find yourself spending less time covering holes if you take a more proactive approach to security than a reactive approach.

### A.5.2 Security and the Local Machine

Security at a local machine can be very easy to maintain. Using a secure operating system such as HP-UNIX Secure OS CMW, UNIX running Secure Shell, or Windows NT on a local machine that is not attached to any network is relatively safe, as long as you follow the installation instructions provided with the operating system on security and "C2" Compliance. Basically, "C2" is covered in the Orange Book, and states that any machine that employs auditing and user access lists can be considered "C2" compliant. Turning off the boot from floppy and requiring a password to change system settings keeps the user from making the machine non-C2 compliant.

When connecting a local machine to the Internet, care should be taken to make sure that all of the security patches are installed, and that no software with security flaws is used that can allow a hacker to damage or destroy settings or data on the machine connected to the Internet. Turn off all services that are dangerous or unnecessary, such as IPX/SPX and NetBEUI protocols, and WINS. Programs such as Microsoft Internet Explorer 3.0 and earlier, or Netscape Navigator 2.02 or earlier, should be upgraded to the latest versions, and F-Prot or some other type of Virus Scanner should be installed to scan downloads for viri. Virus scanner programs may be available from the local IM authority or via downloading from a remote DoD site, if a DoD enterprise licence is required and has been granted.

### A.5.3 Security and Network Planning

If you are running one computer, and accessing the Internet via America Online or some other Internet Service Provider (ISP), you really do not have to worry about network planning. You still have to worry about securing one machine and making sure your users are secure. If you are running a network attached to the Internet and plan on downloading files, it is important to take the necessary security precautions.

Computer networks allow an organization an excellent opportunity to work creatively. Projects can be worked on by several different workers in several different locations at the same time, improving communication between the users. However, networks also pose some serious dangers that are not faced by single computers. Because every computer can communicate with the other computers on the network, users may be able to access information to which they normally would not have access. Networks also allow hackers to mount attacks against several machines, or gain access to multiple sources of information.

Care must be taken when attaching computers to the network. Beyond installing all the necessary bug fixes and security patches to the operating system, special care must be taken to make sure that all software running on each of the systems is relatively safe. Programs with major security flaws, such as Microsoft Internet Explorer 3.0, should be removed from the system entirely, or upgraded to a version that fixes the problem. If the computers on the network are not protected by a firewall, care must be taken to make sure that users are using strong passwords, and that dangerous services are not being used. Services such as NetBEUI and WINS have serious bugs in them that should be turned off until their flaws can be fixed. Computers with static IP addresses are especially vulnerable, since they are available to the outside world whenever the computer is on.

With a network situation, you should check with your ISP to see if they have a firewall installed. If they do not have one installed, or they have a large number of customers who are unknown or untrusted, you should probably set up your own firewall to protect your network from the outside world. Firewalls are covered in more detail below.

### A.5.4 Firewalls

In building construction, a firewall is a wall designed to keep fire confined in one section of the building for a period of time, allowing people within the other sections of the building enough time to escape. In computer terms, a firewall keeps one section of a network confined and away from the dangers of the other sections of the network. It is easier to think of a firewall as a moat and drawbridge around a castle. The moat is designed to keep attackers from climbing the castle walls, while the drawbridge is designed to allow those who are permitted to enter the castle to cross the moat. The moat’s main purpose is to keep unwanted people out, while the drawbridge’s main purpose is to allow wanted people in. A firewall is best defined as a pair of mechanisms designed to keep unwanted people out, and let wanted people in.

To be effective, a firewall must restrict people to entering the confined network via a carefully controlled channel, keep attackers from getting near your internal computers, and restrict people to leaving the confined network via a carefully controlled channel. The firewall will decide what people it should keep out, and what people it should allow in by a set of rules that you supply. If you tell a firewall to let everyone but a small number of people in, it will let everyone but a small number of people in. Likewise, if you tell it to keep everyone but a small number of people out, it will keep everyone but a small number of people out.

The Internet has its share of vandals, crooks, and spies. A firewall can effectively prevent these users from gaining access to machines on your internal network. However, a firewall is only as good as the planning that goes into your network and your access control policies. If your network has any backdoors (dial-in servers, Internet web servers, etc.) or your access control policy is not well planned, a firewall will do little good.

Firewalls are built using several different techniques, but we will only cover one type of firewall, the DoD-Standard Screened Subnet Firewall Architecture, in this document. To get more information on the different types of firewalls, check out the book *Building Internet Firewalls*, and the web-page "Internet Firewalls FAQ" (both references are listed at the end of this document.)

A Screened Subnet Firewall Architecture, as shown in Figure A5, uses two routers and a host computer to operate, though one router and a host computer can be used if funds are limited. The two routers are designated as an external router, which handles traffic from the outside world into the firewall, and an internal router, which handles traffic from the firewall into the inside network. The host computer, often called a Bastion Host, acts as a web server for the outside world, while keeping the amount of damage that could be done by the intruder to the internal network to a minimum.

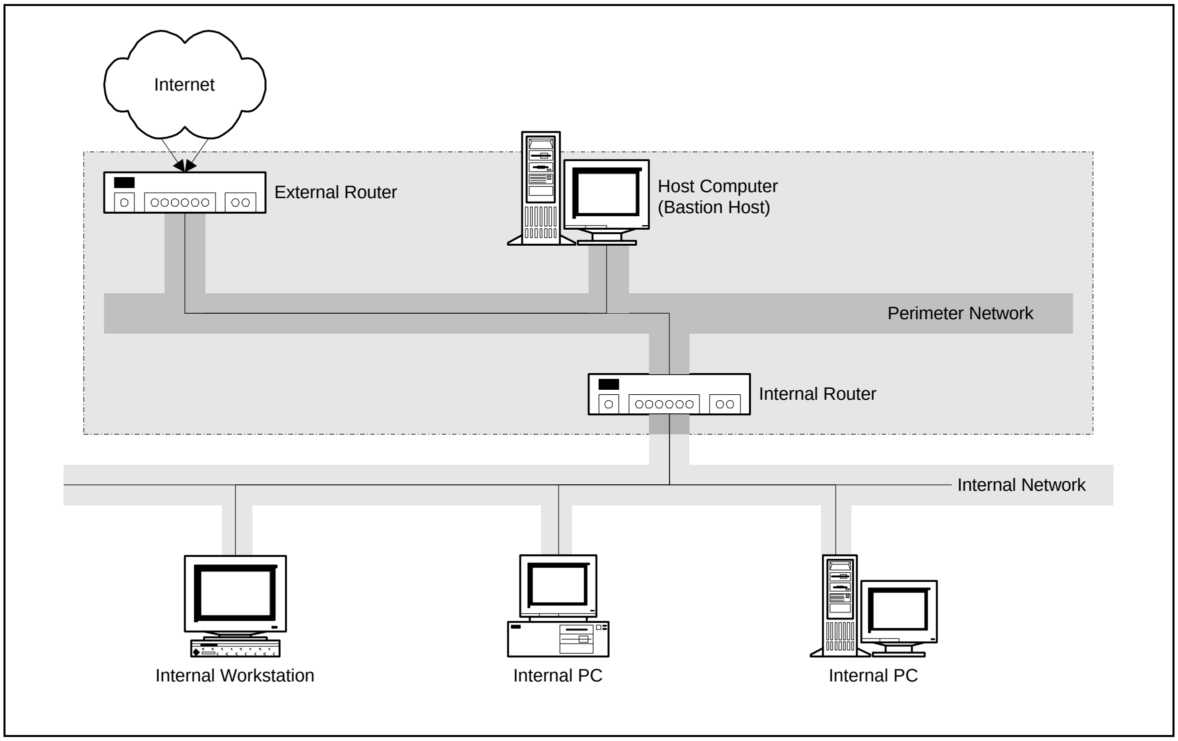


**Figure A5. Screened Subnet Architecture.**

A good way of minimizing the effects of backdoors on an internal network is to put all outside web servers on a perimeter network. These web servers should not be trusted by any of the computers inside your firewall, and should have a minimal number of services running (only the web server software itself, if possible).

## A.6 BIBLIOGRAPHY AND SELECTED RESOURCES

### A.6.1 Webpages and Online Resources

**General Security Sites**

CERT (Computer Emergency Response Team): http://www.cert.org/index.html

COAST Security Archives: http://www.cs.purdue.edu/coast/index.html

FIRST (Forum for Incident Response and Security Teams):
http://www.first.org/index.html

Gene Spafford's Security Links: http://www.cs.purdue.edu/homes/spaf/hotlists/csec.html

UC Davis Security Lab: http://seclab.cs.ucdavis.edu/index.html

**Advisory Information**

CERT Advisories: ftp://info.cert.org/pub/cert_advisories

**Firewall Information**

Trusted Internet Systems (TIS): http://www.tis.com/index.html

**Policy Writing Information**

RFC 1244 - Site Security Handbook Model: ftp://nic.merit.edu/documents/fyi/fyi8.txt

### A.6.2 Magazines and Periodicals

Infosecurity News (ISSN: 1066-7822). MIS Training Institute Press Inc., Call 508-879-9792 or http://www.infosecnews.com for subscription information. ($8 ea./8 issues.)

### A.6.3 Books

Chapman, D. Brent & Zwicky, Elizabeth D., *Building Internet Firewalls.* (ISBN: 1-56592-124-0). O'Reilly & Associates, Inc., 1995.

Pfleeger, Charles P., *Security In Computing.* (ISBN: 0-13-798943-1). PTR Prentice Hall, 1989.

Sheldon, Tom, *Windows NT Security Handbook.* (ISBN: 0-07-882240-8). Osborne, 1997.

# APPENDIX B: NETWORK MANAGEMENT

## B.1 INTRODUCTION

Network management is complex and is usually specific to the Network Operating System chosen during network design and definition. *Networking for Dummies*, provided with this guidebook, has an extensive section (Part III) on the difficulties of the Network Manager's tasking for specific Network Operating Systems. The remainder of this appendix provides, through a description of the ISO Network Management Model, a list of items to consider when managing a network.

## B.2 ISO NETWORK MANAGEMENT MODEL

The ISO Network Management Model helps define network management. The model comprises five specific areas associated with network management:

1. Configuration Management
2. Fault Management
3. Security Management
4. Performance Management
5. Accounting Management

The following sections describe each area.

### B.2.1 Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects of various versions of hardware and software elements on network operation can be tracked and managed. Some hardware and software pieces simply do not work together. Configuration management can in some ways be thought of as "standardization," but it requires more than just standardization (although if everything is the same it might certainly be easier to manage). Configuration management requires a thorough understanding of what you have, and how these things do or do not work together.

The ISO Configuration Management portion of the Network Management Model comprises the following:

- Defining resources and attributes
- Setting/modifying attribute values
- Defining/modifying relationships
- Examining attribute values
- Examining relationships
- Distributing software
- Initializing/terminating network operations
- Verifying user authorization
- Reporting configuration status

Essentially, this process is common sense. If you know what you have and know what is necessary to make your hardware and software work together (patches, bug fixes, etc.), you will have a more successful network.

### B.2.2 Fault Management

The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems in order to keep the network running effectively. We will not address specifically how to do fault management here; instead, we will describe the standard elements. Fault management is the most widely implemented of the ISO network management elements. This makes sense—faults cause downtime for the network. Once you have a network, you will come to rely on it—and rely on it being up.

The Fault Management portion of the ISO Network Management Model comprises the following:

- Detecting and reporting faults
- Diagnosing faults
- Correcting faults

### B.2.3 Security Management

The goal of security management is to control access to network resources according to local guidelines so that the network is resistant to hackers and so that sensitive information cannot be accessed without appropriate authorization. Appendix A (Network Security), describes some of the problems that might occur if you do not manage security.

Security management subsystems work by partitioning network resources into authorized and unauthorized areas. For some users, access to *any* network resources is inappropriate. Such users are usually organizational outsiders. For other network users, access to information originating from a particular workgroup is inappropriate. For example, access to personnel files is inappropriate for most users outside the personnel department. However, proper access does not happen automatically; security policy and implementation are critical to success in security management.

The Security Management portion of the ISO Network Management Model comprises the following:

- Controlling access
- Archiving and retrieving security information
- Managing and controlling encryption process

### B.2.4 Performance Management

The goal of performance management is to measure various aspects of network performance information so that inter-network performance can be maintained at an acceptable level. Some metrics for this include network throughput, user response time, and line utilization. Again, this makes sense. You expect your network to perform well. The metrics or measurements for performance are referred to as performance variables.

Management personnel should continually monitor performance variables. When a performance threshold is exceeded, an alert should be generated and sent to these management personnel.

A network performance management system can be reactive or proactive. In a reactive system, when performance is identified as unacceptable due to exceeding an established threshold, the system reacts by sending a message. Proactive management determines how network growth will affect performance metrics. This process (normally using simulations) can effectively alert administrators to impending problems so that measures can be taken before they result in a performance failure.

The Performance Management portion of the ISO Network Management Model comprises the following:

- Monitoring performance
- Tuning and controlling performance
- Evaluating performance tuning
- Reporting on performance monitoring through tracking
- Testing capacity and special conditions

### B.2.5 Accounting Management

The goal of accounting management is to measure network utilization parameters so that individual or group uses of the network can be regulated accordingly. The ISO standard talks about “fairness” in resource use and management that can be established as a result of accounting management. In essence, however, this accounting management examines resource utilization, down to the user level, and determines if use of the resource is appropriate. If you have limited resources, you will find that once you start to add resources to your network (e.g., color printers), users will automatically rush to use these resources, which may result in bottlenecking or resource hogging. By knowing who is using what on your network, you can tell if the use is appropriate, and whether or not you need to add additional resources to the network.

Accounting management can also be useful when you are sharing the costs of a network. For example, your command might be sharing a network with another command; accounting management can help determine each command’s “fair share” of costs.

The Accounting Management portion of the ISO Network Management Model comprises the following:

- Recording and generating accounting information
- Specifying accounting information to be collected
- Controlling storage and access to accounting information
- Reporting accounting information
- Setting and modifying accounting limits
- Defining accounting metrics

## B.3 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

In this appendix, we have focused on what needs to be done, rather than how it will be done. Many vendors and software packages are available to help you perform network management. Most of these packages are constructed around a “built-in” capability that was introduced in the early days of the Internet, called Simple Network Management Protocol (SNMP), and is therefore compatible with the protocols TCP, IP, and others discussed in this guidebook. The premise of SNMP is to have each network device report information about itself. SNMP also allows the reporting, in addition to basic information, of device-specific data. The combined information from all SNMP sources forms the Management Information Base (MIB).

SNMP operates on a request/response basis, with requests made by the network management server to the SNMP agent on each managed device. Six SNMP operations are defined:

1. Get – allowing the management server to retrieve a piece of information from the SNMP agent
2. GetNext – allowing the management server to retrieve the next piece of information from a table or list within an agent
3. GetBulk (only implemented in SNMPv2) – allowing the management server to acquire large amounts of related information without having to initiate a GetNext
4. Set – allowing the management server to set values for events within an agent (trap) to asynchronously inform the management server of their occurrence
5. Trap – used by the agent to asynchronously inform the management server of some event
6. Inform (only implemented in SNMPv2) – allowing one management server to send trap information to another management server

To implement SNMP, all devices to be managed must be SNMP-compliant. This is not always the case. Further, the MIB, by itself, is not particularly useful to the network manager. A software network manager is required. As mentioned, many vendors and network management software packages are available. The Navy standard is HP OpenView. If you can afford this package, it can provide an excellent tool for performing network management. If you cannot afford it, you should consider one of the many PC-based network management software packages (including some that are built into the Navy standard Windows NT system) that meet your needs. Important considerations (aside from cost) include the ease of implementing the management system on your network and ease of using the system.

# APPENDIX C: NETWORK PLAN FILL-OUT FORMS

This appendix is intended to be used in conjunction with Sections 3.3 and 3.4 of the guidebook to assist in the determination of organization requirements. The appendix consists of a series of fill-out forms. When completed, this appendix will form the organization network plan.

Section C.1 is to be used to assist in the determination of User Expectations. Section C.2 is to be to assist in the determination of the Functional Requirements. Section C.3 is to be used to assist in the Resource and Operating Conditions Assessment. Section C.4 is to be used to assist in Design and Definition Assessment.

**Due to the volatility of component prices a cautionary note needs to be stated. While cost figures are provided herein, the reader is urged to use the latest cost figures, which can be obtained via the contract vehicles provided in Section 4.2 of this guide.**

## C.1 USER EXPECTATIONS

***Instructions: Reproduce the fill-out forms for User Expectations, including the provided cover sheet for your network plan. Fill out all forms and keep them together. A three-ring notebook would be useful for this purpose.***

# NETWORK PLAN

**PREPARED FOR: (COMMAND NAME)__________________________________**

**PREPARED BY:___________________________________________________**

**DATE:**

# WHAT DO WE WANT?

**Check those capabilities/features that your command desires. Also prioritize those capabilities with 1 being the highest priority:**

| Check | Feature/Capability | Priority |
|---|---|---|
| | Electronic Mail (Command Internal Only) | |
| | Electronic Mail (With Naval Community of Users) | |
| | Internet Connection to support WWW Browsing | |
| | Ability to share applications within the command | |
| | Ability to share files and information within the command | |
| | Ability to share printers and other network devices within the command | |
| | A Central Place to Store Files | |
| | An Unclassified (only) Network | |
| | A Classified (only) Network | |
| | A Network Supporting Both Classified and Unclassified | |
| | A Really Secure Network (no hackers please) | |
| | A Really Fast and Responsive Network | |
| | Something Really Easy to Use | |
| | A Network that is Centrally Managed and Administered | |
| | A Network that the individual users can manage and administer | |
| | A Network that operates only during working hours | |
| | A Network that operates around the clock | |
| | A Network that never goes down | |
| | A Network that will support remote or offsite access (from home or on the road) | |
| | A Network that is affordable | |
| | A Help Desk for inexperienced users | |

# WHAT DO WE HAVE?

| | |
|---|---|
| Estimated Number of Users | |

**<u>Numbers of Systems/Peripherals by Type:</u>**

| | |
|---|---|
| UNIX | |
| Macintosh | |
| PC-80286 | |
| PC-80386 | |
| PC-80486 | |
| PC-Pentium | |
| PC-Other | |
| Individual Printers | |
| Network Printers | |
| Other Network Devices | |

**<u>Operating Systems by Type</u>:**

| | |
|---|---|
| UNIX | |
| Macintosh | |
| MS-DOS (Only) | |
| Windows 3.1/3.11 | |
| Windows for Workgroups | |
| Windows 95 | |
| OS/2 | |
| Windows NT Workstation | |
| Windows NT Server | |
| Novell Netware Server | |
| Other NOS Server | |

**<u>Current Applications Standards:</u>**

| **Application** | **Organization/Command** | **Community (Chain of Command)** |
|---|---|---|
| Word Processing | | |
| Spreadsheet | | |
| Presentation | | |
| Database | | |
| Groupware | | |
| Electronic Mail | | |

# MORE ABOUT OUR COMMAND

**Some additional things we might want in the future (check the ones that apply):**

| | |
|---|---|
| | Large file exchange (Files larger than 10 Mb such as large presentations or graphics) |
| | Mapping |
| | Dial Up Services (to support telecommuting or remote/offsite information exchange) |
| | Voice and Video (Desktop Video Teleconferencing) |
| | Web Server |
| | Groupware |
| | Firewall for additional security |

**Training/Proficiency Level for Users, Installers, and Network Managers:**

| Users | Installers | Net Managers | Training/Proficiency |
|---|---|---|---|
| | | | Well Trained and Skilled |
| | | | OK, But needs a little care and feeding |
| | | | Marginal and needs a LOT of care and feeding |
| | | | Computer and Network Illiterate |

**Who I have talked to so far:**

| | |
|---|---|
| | Host/Base Communications Officer (to find out if there is an existing base network, how to tie in, and the nearest Service Delivery Point or Base Interconnect Point) |
| | Other commands in the local area that have networks |
| | Other commands in the chain of command that have networks |
| | Local NCTS |
| | Local DISA |
| | Local Facilities Manager (To see if there are local instructions or procedures to follow) |
| | Local Public Works Center (If you have multiple buildings in the command you might have to trench. They can tell you what rules need to be followed) |

## C.2 FUNCTIONAL REQUIREMENTS

### C.2.1 Functional Requirements

This is a distillation of things you have provided under User Expectations. It is a good idea to have the main guidebook open as you go through this section, and to have blank pages in your network plan to write down your questions, answers, and concerns. As issues are raised, you need to examine the relevant sections of the guidebook, and write down information.

The first part of this section is a fill out form and narrative discussion that generates requirements. The final part of the section is the process data flow diagrams for Functional Requirements. Include the fill out forms and highlighted narrative discussion in your network plan.

# FUNCTIONAL REQUIREMENTS FILL-OUT FORM

**Review your choices of what you want and put them in order of priority. List below your top five selections:**

Priority 1 :

Priority 2 :

Priority 3 :

Priority 4  :

Priority 5:

The cost factors relevant to putting together your LAN will be covered in the Design and Definition Phase of this Network Plan.

The reason for prioritizing your expectations is to focus on what is most important, so if choices need to be made, you can weigh options against what you really want. When reviewing the implications of your choices, it is also advisable to indicate any additional equipment that might be required to achieve your priorities. This will assist you, in the Design and Definition Phase of the process, to make decisions concerning costs required to implement. You need to note any additional cost items (indicated by an asterisk (*) in the narrative discussion), and to transpose those items/costs to the Design and Definition fill out forms.

## C.2.2 Required Components Based Upon Your Choices

**If Electronic Mail is one of your choices, you will need the following:**

1. LAN
2. *A mail server (This might be an additional Cost Factor)
3. *Mail software (This might be an additional Cost Factor)
4. Unique mail addresses for each user
5. *A gateway that connects the mail server to the Internet (SMTP or X.400 are common) (This might be included in your Mail Server Software Package, but check)
6. *A Domain Name and Domain Name Server (This might be an additional cost factor for a Server)

Since DoD migrating to DMS, your mail software must be DMS compliant.

**If Internet Connection is one of your choices, you will need the following:**

1. *An Internet Service Provider (This will have recurring and setup costs)
2. TCP/IP addresses (Provided by the Internet Service Provider)
3. *A Domain Name and Domain Name Server (The Server is a Cost Item)
4. *TCP/IP software for each user machine (Depending on what Operating System you are using, there may be a cost incurred here)
5. *FTP, TELNET, WWW Browser Software for each user machine (same as #4)
6. *Virus Protection Software for each user machine (There will be a cost here unless you use a product for which DoD has an enterprise licence).
7. *A Firewall (highly recommended) (There will be a significant cost here for server, software, and setup)

**If resource sharing is one of your choices, you will need the following:**

1. *A Network Operating System (Depends on what Operating System you have)
2. *Capability for the network to interact with shared network devices (this can be provided by the right Network Operating System)

**If someone to manage the network is one of your choices, now is not to early to start grooming your resources.**

If you are a large shore based command, you should consider hiring someone (civilian or contractor) to do the management function. This provides long term continuity. If you want to home-grow a network manager, there are many courses out there. As a minimum, you should have someone take a system administration course for the particular Network Operating System that you select. A manufacturer generic router course (one for the specific router you choose for your site), and a general network course is also helpful. If there is another command in the area that already has a network, you can also ask them how they handle things. This might also be an entry into connecting to their network, if they are doing things that you might like to do. There is a caveat when you take the advice of your neighbors, which is that you have to remember that this is your network, filling your requirements and built to your specifications. What makes sense for them might not particularly make sense for you! (There will be training costs associated with this selection.)

Enlisted personnel should look into the Information Systems Administrator (ISA) course taught by Chief of Naval Education and Training (CNET). It should be stressed that the person appointed to administer the LAN should be dedicated and enthusiastic about the position. This position should not be a collateral duty.

It is critical that chain of command (FLTCINC) procedures be followed to ensure  that you are following their standards.  things are going in the right direction.

**If Help Desk is one of your choices, this is very much like someone to manage your network.**

Now is not too early to start grooming this capability. Something as simple as a book of instructions. A "frequently asked questions (FAQ) list", might suffice. You will be making up this guide as you go along, as it becomes your "brain book." (Training Costs will be incurred)

**If Unclassified (Only) Network is one of your choices, you will need the same type of stuff as for an Internet connection.**

Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) also applies here. NIPRNET provides unclassified network connectivity for all DoD agencies.

**If a Place to Store Files is one of your choices, you need to invest in server(s) storage capacity.**

When planning, you also need to consider redundancy, access speed, and reliability. Unlimited capacity doesn't really provide any benefits if you can't get to it because of a system failure. (There will be equipment costs).

***If Classified (Only) Network is one of your choices, you will need the same type of stuff as for an Internet connection.**

A Classified network is very complicated to install and requires strict adherence to a variety of security instructions. If it is truly a requirement, you should obtain the services of DISA To connect with other classified networks, you will want to consider obtaining access through the DISA classified network known as the Secret Internet Protocol Network (SIPRNET)

**If a Network Supporting Both Classified and Unclassified is one of your choices, you will need a lot of help.**

Under current instructions, since there is no approved method for interconnecting secure and unclassified networks it is a requirement that they be kept separate. The current state of technology does not support this type of capability, and it is not a recommended course of action to interconnect these LANs. Salvation may be coming in the future with the Defense Message System's MISSI (Multi-Level Information Systems Security Initiative) MLS (Multi-Level Secure) software and hardware. It is recommended that DISA be consulted.

**If a Really Fast Network is one of your choices, i.e., performance is a concern, then you need to pay particular attention to the way the network is engineered up, and remember the old adage that the "bottleneck usually lies at the top of the bottle."**

Of course it's generally not a problem until you turn the bottle over, i.e., until you really need to use what's in the bottle. If you read the sections of this guidebook pertaining to wiring, and ensure that all of your plumbing and equipment supports fast ethernet or better, you will have a fast internal network. Pay attention to the connection to the service provider (which is a potential bottleneck).

**If Something Easy to Use is one of your choices, you need to pay particular attention to the current skill level of your users.**

In most cases, change is a very frightening thing to mandate. Ease of Use is an issue normally relating directly to the Network Operating System. You need to step away from your role as Network System Engineer and put yourself in the position of a user on the network. You need to pay particular attention to "look and feel" issues for the users, and what specific changes in their behavior will be required to use the network. The same goes for network management.

**If Something Else is one of your choices, you may need to obtain consultation services if your annotation is not found in the discussion below:**

- Something that I can grow into over time (start small and get bigger), or something that I will not require a forklift to upgrade in the future. {Note: a "forklift upgrade" is a derogatory term for a low capability network that requires everything to be replaced – hence the term "forklift" in order to improve the network}. If you pay attention to the guidelines and what is on the horizon, you should be able to carry your network well into the future. Planning, Planning, Planning.

- Something that is affordable. We, of course, do not know what your funding situation is, but have included in this guideline sufficient information to allow you to estimate what the network will cost in FY97 dollars (along with options for comparison). In today's world, cost is more than likely to be the driver in most decisions, and we are sensitive to this reality. Our advice is to spend a lot of time in cost comparisons, and be aware of the implications of any decisions on costs. Make at least two passes on costing. The first pass should be a system that fills all of your requirements (Cadillac System). The second pass should be a system that fills only the top priority or priorities. In order to keep from creating a system that will require "forklift upgrades" you need to focus on how to migrate from what you can afford based upon your priorities to what you really need.

- Really reliable network. Put a lot of attention on redundancy and proactive network management tools. Consider "dual homing" as an option. In essence, this creates two discrete paths from your priority resources to anywhere in the network, thus decreasing the possibility of total failure for network components. Also consider extensive backing up of network storage devices, and "striping" or "mirroring" these storage devices. When designing redundancy in your network, do not forget the path from your network to the outside network. A cheap way to provide redundancy is to implement a second link to your service provider, which could be an ISDN or lower speed modem connection. If the primary link is lost, this alternate link kicks in, and you are still on the air (albeit at a lower bandwidth). Under normal circumstances you are paying only for the lease of the second link (but not for the usage). In the event of primary link failure, you pay for the usage of the alternate link (which is normally a higher rate than the primary link). Hopefully this will be for only a limited period of time until the primary link is restored. Your service provider should be able to suggest alternative strategies and costs for this service.

Now you have completed the distillation of what you need, and should have a clearer picture of your requirements. Now you can look at what you have, and see how this will impact your needs.

## C.3 RESOURCES AND OPERATING CONDITIONS ASSESSMENT (ROCA)

In this section you will be collecting far more specific information about your network, and will be making some initial networking diagrams to be used in the Design and Definition Phase. The information you will be collecting will specifically be used for determining a cost estimate for the network, so it is important to be thorough in your data collection. For the fill out form, you will need to have one sheet for each user, which should be included in your network plan.

### C.3.1 ROCA Fill Out Forms

The following pages are the necessary forms to complete the Resources and Operating Conditions Assessment.

# ROCA USER INFORMATION FORM

**User Name: ___________________________________________**

**User Location:**

**Building Number: ____________**
**Floor: ____________**
**Room: ___________**

**Location Sketch (Include Measurements):**

**User Equipment:**

Computer Type ____________________
Operating System __________________
Network Interface Card Required? Yes No
Additional Devices: Printer _____________ Network Printer ________________
Is there a specific workgroup this user will be assigned to? Yes No ____________

**Installed Applications:**

---

**New Applications Required:**

List Them:

---

**New Computers Required?**

How Many?

# ROCA BUILDING INFORMATION FORM

## (Reproduce for Number of Floors in the building – 1 each)

**Building Number: ____________________**

**Number of Users in the Building: _________________**

**Number of Floors in the Building: ________________**

**Location and dimensions of Wiring Closet for each floor: _________________________**

**Sketch a floor plan for each floor (include dimensions if possible). Include User Office and Wiring Closet
Locations.**

**Are there hung ceilings or raised floors on this floor? Yes No**

**Existing and Available Cable routes for this floor/building:**

# ROCA BUILDING-TO-BUILDING INFORMATION FORM

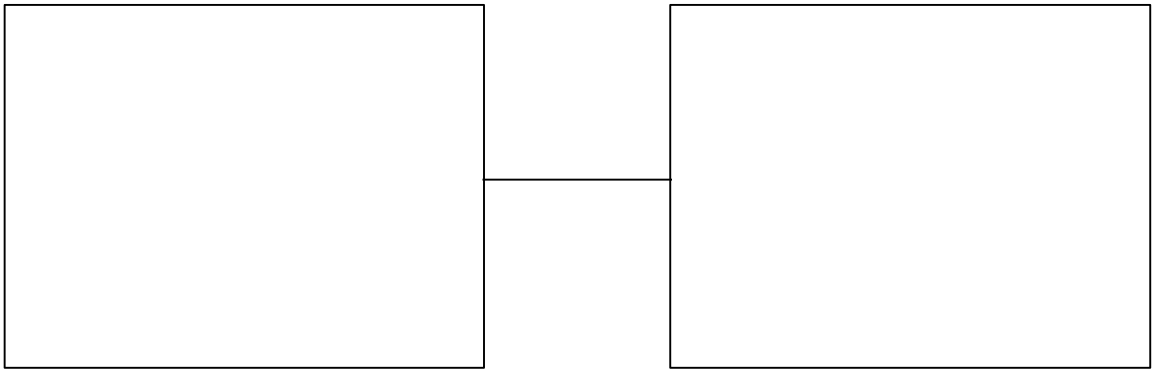
**For Building _________ to Building ___________**

**Distance between buildings: ______________________________**

**Description of terrain between buildings (include parking lots, roads, etc.).**

---

**Building-to-Building Sketch (including measurements):**



---

**Location of Connection Points for Each Building:**

---

**Existing and Available routes for Cable/Fiber:**

# ROCA IN HOUSE SKILL LEVEL FORM

**Names and skill levels of personnel in the following disciplines:**

**Equipment Installation and Setup (include computer equipment and network equipment – NICS/Routers, etc.):**

**Network cabling Installation and Setup (include cable pulling, installation of wall jacks, etc.):**

**Equipment and Network Maintenance (repair of network equipment):**

**Network Management (administration and management of network operating system):**

**Applications Experts (for help desk functions):**

## C.4 NETWORK DESIGN AND DEFINITION

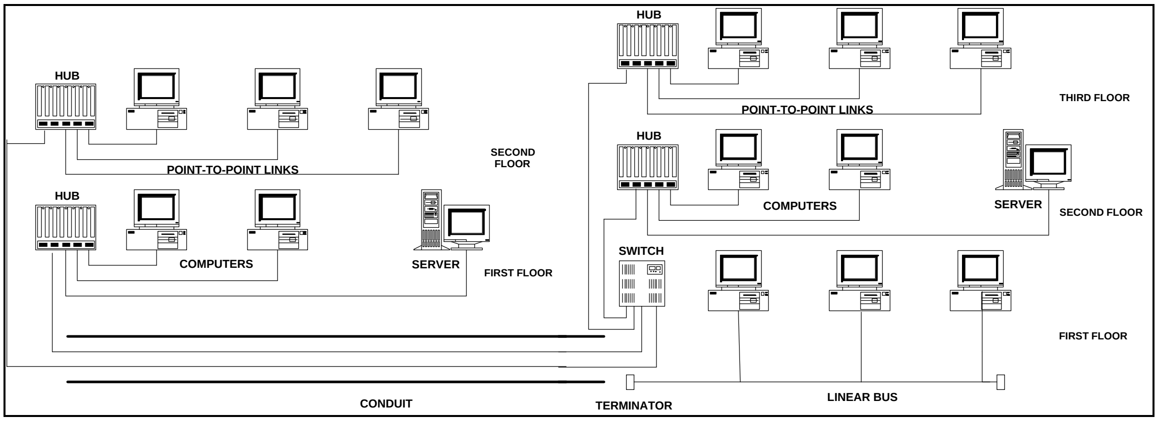
It is important that you talk extensively with the Base Communications Officer (BCO), the local NCTS, DISA representative, and other commands in your area that have networks, to determine connection options. Determine the location of their Service Delivery Point (SDP) or Base Interface Point (BIP). You will also want to ask them if there are any recurring connection fees, when they should be paid), and any equipment that will be required for you to connect to these (sometimes a CSU/DSU (Channel Service Unit/Data Service Unit)is required to convert the output of the connection to an input to your connection device – normally a router at your site). Also, determine if you are responsible for arranging any Local Exchange Carrier (LEC) provided connection circuits within your LATA (Local Access and Transport Area) (which will require a Telecommunications Service Request (TSR), and lease with the local LEC).

The Network Design and Definition Process is iterative. Your first pass through the information will provide you with a ballpark estimate for what you want and need. You can then compare this with your budget to determine if you have a good fit. It is important to try and get your initial estimates as “right as possible”. If your initial estimate is out of balance with your budget, you need to focus on your priorities, and fill those requirements first (that is why this is an iterative process).

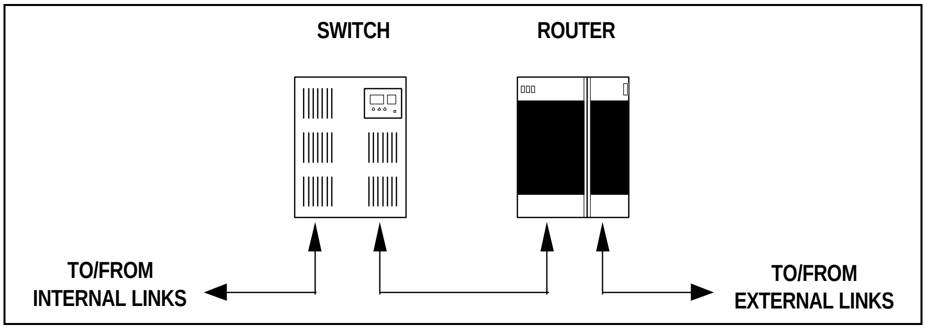
The initialization will get you in the ballpark, but it is important to get as accurate as possible as you progress with each iteration. This guide provides a listing of existing contract vehicles (see Section 4.2), that can give you pricing information on specific equipment and services you require.

During the process, it will be helpful to have in front of you some of the figures from the basic document, which will save you time in coming up with a good draft configuration for use in your network plan. We have included these figures in the fill out forms for this section.

Figures 6 and 7 from the basic document are included for your modification to fit your situation.



**Representative Inter-Building LAN Configuration.**



**Internal/External Link Connectivity.**

These two figures show inter-building and internal/external connectivity, which are two major areas in your network plan. Cut and paste these figures as required to come up with a good and annotated representation of your network. Note that cost figures change rapidly. Figures provided in this document are based on fourth quarter 1997 figures and should be adjusted as appropriately.

## RULES OF THUMB FOR ESTIMATIONS

### Router

See the description of routers in the text. A basic cost for a good router is $18K. A FDDI network interface is $12K. An ATM network interface is $17K. A 6-port ethernet interface card is $12K. We recommend only using 5 out of the 6 ports. Keep the sixth one for a spare or for future growth. Prices, port configurations, numbers of slots available and capability vary greatly from company to company. The fewer the number of users, the higher the cost per user. If you know enough about your current situation, you can itemize, but a good rule of thumb for router cost is about $70/user.

### Etherswitch

The etherswitch is a network device that helps control loading on a network segment. The switch will not forward all traffic down all attached segments. It forwards only to the segment that the packet's destination device is attached. Costs vary based on capability and number of ports depends upon the manufacturer. The range is from $5K to $40K. Taking an average, 10 port switch, the cost per user is $85. With assignment:

- 6 ports for hub attachment
- 1 port for server attachment
- 1 port for router connection
- 2 ports for spares

**ATM Device**

If you are connecting to an ATM backbone, you may be required to purchase a switch (in some cases it might be included in the service, but you need to ask). You need to check the current market to determine the actual cost of a switch.

**Building Wiring**

This applies to the wiring inside the building. This is the hardware that goes from the wall plate to the central wiring closet(s). The number of wiring closets will depend upon the size and layout of a building. The components are:

- $50/user for miscellaneous connectors, wire, CAT5 cable, wall boxes, patch panels, patch panel rack, etc.

- $90/user for installation of the above. For both of these a minimum of 20 people is assumed. If you do this by 1s and 2s it can be a cost killer.

**Hubs**

This is for a 24-port SNMP manageable 10BaseT hub. This is based on connecting 20 people to a hub. The hub costs approximately $1200. Port use is as follows:

- 20 user ports
- 1 port for server
- 1 port for router
- 2 spares

$10 per user for a fully loaded hub. We recommend putting more hubs in for future growth. You can get hubs with 12, 24, 36, 48, etc. ports. From a network design perspective and to keep network loading down connecting a maximum of 20 people per hub is a good idea.

Consider $15-20/user for a 100BaseT Hub for estimation purposes.

**Physical Factors Cost Estimation**

Physical layer cost model - external plant, i.e. cable and conduit between buildings

Plant installation cost varies with the following factors:

**Distance -** a run with constant parameters (all other factors remain the same) will cost less per unit as the distance increases. As in any other endeavor, quantity brings the price down and this applies directly to conduit/cable installation.

**Building entries -** the number and complexity of the building entry is the most variable factor. This factor is highly variable because every building is different. New buildings generally have cable entry designed and built into the building where older buildings don't. Also the building structure has an effect on ease of entry. It is significantly less expensive to provide an opening in a wood framed building than it is in a concrete structure. Think of adding to a gun bunker in this case.

**Topology -** topology varies from virgin soil to a highly industrialized well traveled, street. In the first instance, it is just trenching through dirt and rock without any manmade obstacles where in the second case there would be existing conduits, pipes, roadway and sidewalks to contend with.

**Configuration -** the configuration can vary from a single direct buried cable to a multiple conduit bank with interduct and cable glides. Also the back fill involved can vary from just recovering with dirt to concrete slurry encasement with roadway/sidewalk repair.

Several communications installation companies were surveyed and the cost model reflects the general consensus of these companies. The model is based on a 4 inch conduit bundle with interduct and fiberglide covered with slurry. The statistical average cost is approximately $88 per lineal foot. The cost for virgin soil is $50 per foot with the maximum being $150 per foot for short runs into complex building entries. To provide a rough order of magnitude for estimation, a cost of $100 per foot can be used to reflect all factors relating to the Physical Factors Cost Estimation

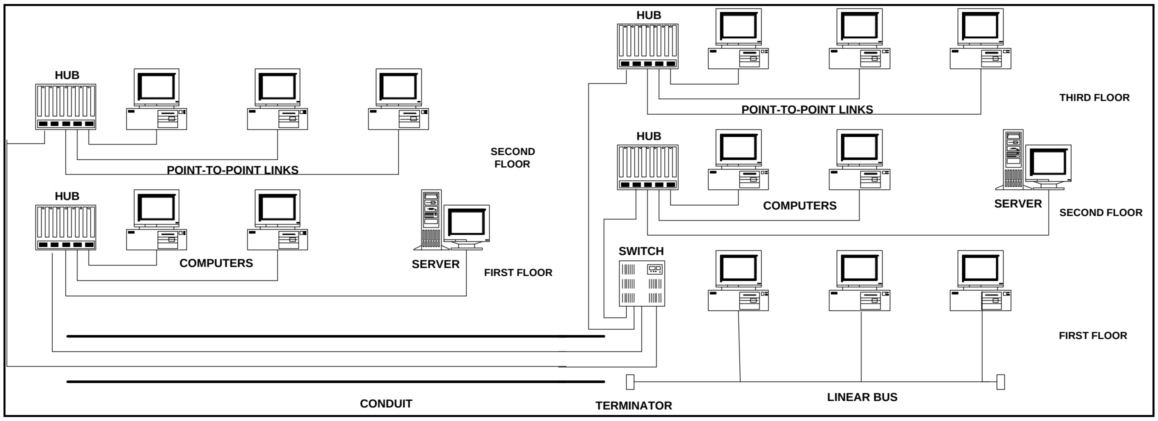
.

Congratulations, you now have enough rules of thumb to deal with for the real tough cost estimating. As with any rule of thumb, it provides an order of magnitude estimate that can be refined later.

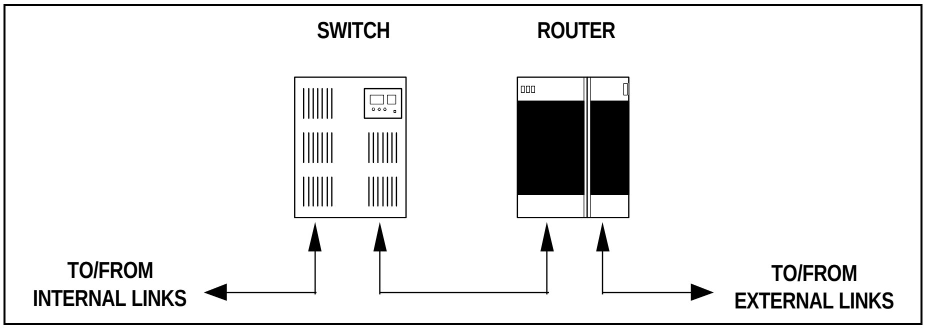
Armed with your ROCA user studies, you can put together some rough-cuts, refining your estimates as you iterate. Remember that these are just estimates. You will need to refine these estimates based upon gaining specific cost information from various sources. Section 4 of the Network Guidebook, and in particular Table 6, will give you resources and sources of information on existing contracts that will help you refine your estimates. You now have enough information to pursue this phase.

## Definition and Design Fill-Out Forms

Figures 6 and 7 from the main document are included for your modification to fit your situation.



**Representative Inter-Building LAN Configuration.**



**Internal/External Link Connectivity.**

These two figures show inter-building and internal/external connectivity, which are two major areas in your network plan.

## Rule Of Thumb Initial Cost Estimate

| Factor | Rate | Numbers | Total |
|---|---|---|---|
| Router | $70/User | | |
| ATM device (if needed) | Market | | |
| Building Wiring | $140/user | | |
| Hubs | $20/user 100BaseT | | |
| Physical Factors | $100/foot | | |
| Total this Table | | | |

Additional Cost Items from Resources and Operating Conditions Assessment Section:

Priority Requirement #1 $_______________
Priority Requirement #2 $_______________
Priority Requirement #3 $_______________
Priority Requirement #4 $_______________
Priority Requirement #5 $_______________

Other Cost Factors (additional Costs or Costing Refinement):

**Q 1. Would each person in the organization require a desktop computer?**
**Q 2. How many desktop computers will be required?**
**a Itemize by building.**
**Q 3. How many new desktop computers will be procured?**
**a) Itemize these.**
**b) Determine cost for these items.**
**Q 4. How many NICs will be required?**
**Q 5. What application software must be procured?**
**a) E-mail?**
**b) Web Browser?**
**c) File Transfer?**
**Q 6. What supporting application hardware must be procured?**
**a) Mail server?**
**b) DNS host?**
**c) File server?**
**Q 7. How would these computers be spread out in the area that the organization occupies?**
**a) Within a single building?**
**b) Within more than one building? How many?**
**c) What is the physical distance between each pair of buildings?**
**d) Do conduits exist for routing between buildings?**
**Q 8. What are the relative distribution of users within each building?**
**a) Clustered?**
**b) Distributed?**
**c) Both?**
**d) Estimate of linear feet of media required.**
**Q 9. Wall Jacks?**
**Q10.-What supporting hardware will be required?**
**a) Switches**
**a) Port capacity**
**b) Routers**
**a) External**
**b) Internal**
**c) Hubs**

**Add these items that relate to additional costs to the previous thumb rule estimation and you will get a gross estimate of cost.**

**Cost of our Network ______________________**

**Cost Refinement and Specificity**

**Complete a wiring diagram before doing this.**

**Cost Tabulation**

| **Item** | **Nomenclature** | **Quantity** | **Cost Per Item** | **Total Cost** |
|---|---|---|---|---|
| 1. Computers | | | | |
| 2. NICs | | | | |
| 3. E-mail Software | | | | |
| 4. Web Browser | | | | |
| 5. File Transfer | | | | |
| 6. Mail Server | | | | |
| 7. File Server | | | | |
| 8. DNS Host | | | | |
| 9. Building Cable/Building: | | | | |
| a. Wall Plate to Wiring Closet | | | | |
| b. Computer to Wall Plate | | | | |
| c. Floor to Floor | | | | |
| 10. Building to Building Cabling | | | | |
| 11. Switches | | | | |
| 12. Routers | | | | |
| a. External | | | | |
| b. Internal | | | | |
| 13 Hubs | | | | |

| | |
|---|---|
| **TOTAL COST** | |

# APPENDIX D: SCENARIO EXAMPLE

# FOR NETWORK PLAN FILL-OUT FORMS

## NETWORK PLAN

**PREPARED FOR: (COMMAND NAME)_*Flag Command*______________**

**PREPARED BY:________*Aide*________________________________**

**DATE: *Today***

# WHAT DO WE WANT?

**Check those capabilities/features that your command desires. Also prioritize those capabilities with 1 being the highest priority:**

| Check | Feature/Capability | Priority |
|---|---|---|
| | Electronic Mail (Command Internal Only) | |
| X | Electronic Mail (with Naval Community of Users) | 1 |
| | Internet Connection to Support WWW Browsing | |
| | Ability to Share Applications within the Command | |
| | Ability to Share Files and Information within the Command | |
| X | Ability to Share Printers and Other Network Devices within the Command | 2 |
| | A Central Place to Store Files | |
| | An Unclassified (Only) Network | |
| | A Classified (Only) Network | |
| | A Network Supporting Both Classified and Unclassified | |
| | A Really Secure Network (No Hackers Please) | |
| | A Really Fast and Responsive Network | |
| X | Something Really Easy to Use | 4 |
| | A Network that is Centrally Managed And Administered | |
| X | A Network that the Individual Users Can Manage And Administer | 3 |
| | A Network that Operates Only During Working Hours | |
| X | A Network that Operates Around the Clock | 5 |
| | A Network that Never Goes Down | |
| X | A Network that will Support Remote or Offsite Access (from Home or on the Road) | 6 |
| | A Network that is Affordable | |
| | A Help Desk for Inexperienced Users | |

# WHAT DO WE HAVE?

| | |
|---|---|
| Estimated Number of Users | 30 |

**Numbers of Systems/Peripherals by Type:**

| | |
|---|---|
| UNIX | 0 |
| Macintosh | 1 |
| PC-80286 | 1 |
| PC-80386 | 1 |
| PC-80486 | 7 |
| PC-Pentium | 5 |
| PC-Other | |
| Individual Printers | 5 |
| Network Printers | 2 (1 color/1 B&W desired) |
| Other Network Devices | |

**Operating Systems By Type:**

| | |
|---|---|
| UNIX | 0 |
| Macintosh | 1 |
| MSDOS (Only) | 1 |
| Windows 3.1/3.11 | 1 |
| Windows for Workgroups | 7 |
| Windows 95 | 5 |
| OS/2 | 0 |
| Windows NT Workstation | 0 |
| Windows NT Server | 0 |
| Novell Netware Server | 0 |
| Other NOS Server | 0 |

**Current Applications Standards:**

| **Application** | **Organization/Command** | **Community (Chain of Command)** |
|---|---|---|
| Word Processing | WordPerfect | MS Word 6.0 |
| Spreadsheet | Lotus 1,2,3 | MS Excel |
| Presentation | None | MS Powerpoint |
| Database | Dbase IV | MS Access |
| Groupware | None | Lotus Notes |
| Electronic Mail | None | CC:Mail |

# MORE ABOUT THE COMMAND

**Some additional things we might want in the future (check the ones that apply):**

| | |
|---|---|
| X | Large File Exchange (Files Larger than 10Mb such as Large Presentations Or Graphics) |
| | Mapping |
| | Dial Up Services (to Support Telecommuting or Remote/Offsite Information Exchange) |
| X | Voice and Video (Desktop Video Teleconferencing) |
| X | Web Server |
| | Groupware |
| | Firewall for Additional Security |

**Training/Proficiency Level for Users, Installers, and Network Managers:**

| Users | Installers | Net Managers | Training/Proficiency |
|---|---|---|---|
| X | | | Well Trained and Skilled |
| | X | | OK, but need a little care and feeding |
| | | X | Marginal and need a LOT of care and feeding |
| | | | Computer and network illiterate |

**Who I have talked to so far:**

| | |
|---|---|
| X | Host/Base Communications Officer (to find out if there is an existing base network, how to tie in, and the nearest Service Delivery Point or Base Interconnect Point) |
| X | Other commands in the local area that have networks |
| | Other commands in the chain of command that have networks |
| | Local NCTS |
| | Local DISA |
| X | Local Facilities Manager (to see if there are local instructions or procedures to follow) |
| | Local Public Works Center (If you have multiple buildings in the command you might have to trench. They can tell you what rules need to be followed) |

# FUNCTIONAL REQUIREMENTS FILL-OUT FORM

**Review your choices of what you want and put them in order of priority. List below your top five selections:**

Priority 1: Electronic Mail

Priority 2: Share Printers and Network Devices (Color & B&W Printer)

Priority 3: User Managed/Administered Network

Priority 4: Something Really Easy to Use

Priority 5: Round the Clock Operation

Not surprisingly, you will need a Local Area Network for all of these selections.

The reason for prioritizing your expectations is to focus on what is most important, so if choices need to be made, you can weigh options against what you really want.

**<u>If Electronic Mail is one of your choices, you will need the following:</u>**

1. LAN
2. *A mail server (This might be an additional Cost Factor)
3. *Mail software (This might be an additional Cost Factor)
4. Unique mail addresses for each user
5. *A gateway that connects the mail server to the Internet (SMTP or X.400 are common) (This might be included in your Mail Server Software Package, but check)
6. *A Domain Name and Domain Name Server (This might be an additional cost factor for a Server)

**<u>If Internet Connection is one of your choices, you will need the following:</u>**

1. *An Internet Service Provider (This will have recurring and setup costs)
2. TCP/IP addresses (Provided by the Internet Service Provider)
3. *A Domain Name and Domain Name Server (The Server is a Cost Item)
4. *TCP/IP software for each user machine (Depending on what Operating System you are using, there may be a cost incurred here)
5. *FTP, TELNET, WWW Browser Software for each user machine (same as #4)
6. *Virus Protection Software for each user machine (There will be a cost here)
7. *A Firewall (highly recommended) (There will be a significant cost here for server, software, and setup)

**<u>If Resource Sharing is one of your choices, you will need the following:</u>**

1. *A Network Operating System (Depends on what Operating System you have)
2. *Capability for the network to interact with shared network devices (this can be provided by the right Network Operating System)

*If Someone To Manage The Network is one of your choices, now is not to early to start grooming your resources. If you are a large shore based command, you should consider hiring someone (civilian) to do the management function. This provides long term continuity. If you want to home-grow a network manager, there are many courses out there. As a minimum, you should have someone take a system administration course for the particular Network Operating System that you select. A manufacturer generic router course (one for the specific router you choose for your site), and a general network course is also helpful. If there is another command in the area that already has a network, you can also ask them how they handle things. This might also be an entry into connecting to their network, if they are doing things that you might like to do. There is a caveat when you take the advice of your neighbors, which is that you have to remember that this is your network, filling your requirements and built to your specifications. What makes sense for them might not particularly make sense for you! (There will be training costs associated with this selection)

*If Help Desk is one of your choices, this is very much like someone to manage your network. Now is not too early to start grooming this capability. Something as simple as a book of instructions (Network Geeks call this a “frequently asked questions (FAQ)” list, might suffice. You will be making up this guide as you go along, as it becomes your “brain book.” (Training Costs will be incurred)

If Unclassified (Only) Network is one of your choices, you will need the same type of stuff as for an Internet connection. NIPRNET applies here.

*If a Place to Store Files is one of your choices, you need to invest in server(s) storage capacity. When planning, you also need to consider redundancy, access speed, and reliability. Unlimited capacity doesn’t really provide any benefits if you can’t get to it because of a system failure. (There will be equipment costs).

*If Classified (Only) Network is one of your choices, you will need the same type of stuff as for an Internet connection, however you will require cryptographic devices, and your service provider will be DISA, through something called SIPRNET. A classified network is not something that you should do yourself, due to the extensive numbers of regulations that must be followed.

*If a Network Supporting Both Classified and Unclassified is one of your choices, we need to talk. Under current instructions, this is a hard (but not impossible) thing to do, but it requires a lot of money and strict attention to detail. The current state of technology does not support this type of capability, and it is not a recommended course of action (please keep classified and unclassified networks separate, at least until approved technology catches up). Salvation may be coming in the future with Defense Messaging System, which is a replacement for the current AUTODIN system, but we are still a considerable distance from implementation. For now, our guidance is to keep them separate, and for classified networking, talk to DISA to determine how to go about setting up your network.

*If a Really Fast Network is one of your choices, you need to pay particular attention to the way the network is wired up, and remember the old adage that the “bottleneck usually lies at the top of the bottle”. And of course it’s generally not a problem until you turn the bottle over, i.e., until you really need to use what’s in the bottle. If you read the sections of this guidebook pertaining to wiring, and ensure that all of your plumbing and equipment supports fast ethernet or better, you will have a fast internal network. Pay attention to the connection to the service provider (which is a potential bottleneck).

If Something Really Easy to Use is one of your choices, you need to pay particular attention to the current skill level of your users. In most cases, change is a very frightening thing to mandate. Ease of Use is an issue normally relating directly to the Network Operating System. You need to step away from your role as Network System Engineer and put yourself in the position of a user on the network. You need to pay particular attention to “look and feel” issues for the users, and what specific changes in their behavior will be required to use the network. The same goes for network management.

If Something Else is one of your choices, you may need to obtain consultation services if your annotation is not found in the discussion below:

- Something that I can grow into over time (start small and get bigger), or something that I will not require a forklift to upgrade in the future. {Note: a "forklift upgrade" is a derogatory term for a low capability network that requires everything to be replaced – hence the term "forklift" in order to improve the network}. If you pay attention to the guidelines and what is on the horizon, you should be able to carry your network well into the future. Planning, Planning, Planning.

- Something that is affordable. We, of course, do not know what your funding situation is, but have included in this guideline sufficient information to allow you to estimate what the network will cost (along with options for comparison). In today's world, cost is more than likely to be the driver in most decisions, and we are sensitive to this reality. Our advice is to spend a lot of time in cost comparisons, and be aware of the implications of any decisions on costs. Make at least two passes on costing. The first pass should be a system that fills all of your requirements ("Cadillac System"). The second pass should be a system that fills only the top priority or priorities. In order to keep from creating a system that will require "forklift upgrades" you need to focus on how to migrate from what you can afford based upon your priorities to what you really want and need.

- Really reliable network. Put a lot of attention on redundancy and proactive network management tools. Consider "dual homing" as an option. In essence, this creates two discrete paths from your priority resources to anywhere in the network, thus decreasing the possibility of total failure for network components. Also consider extensive backing up of network storage devices, and "striping" or "mirroring" these storage devices. When designing redundancy in your network, do not forget the path from your network to the outside network. A cheap way to provide redundancy is to implement a second link to your service provider, which could be an ISDN or lower speed modem connection. If the primary linkage is lost, this alternate link kicks in, and you are still on the air (albeit at a lower bandwidth). Under normal circumstances you are paying only for the lease of the second link (but not for the usage). In the event of primary link failure, you pay for the usage of the alternate link (which is normally a higher rate than the primary linkage), and hopefully this will be for only a limited period of time until the primary link is restored. Your service provider should be able to suggest alternative strategies and costs for this service.

Now you have completed the distillation of what you want, and should have a clearer picture of what your requirements are. Now we need to look at what you have, and see how this will impact your needs.

**<u>Additional stuff we will need by priority requirements:</u>**

**Priority 1:**

- Email and Internet Connection
- Mail Server: Cost: $6K (Pentium 100 with 6GB storage)
- Mail Software: Cost: Cost of MS Exchange Server Software and 30 Client Licenses
- Gateway: Cost: Not Required, included in MS Exchange
- Domain Name Server: Cost: $4K (Pentium 100) running Windows NT 4.0 Server
- Internet Service Provider: Cost: Connection fees $1500/month for T-1 ($18,000/year recurring) lease from TELCO: $800/month ($9,600/year recurring)
- Virus Protection Software Cost: Site License for $30 per user ($900)
- Firewall Server/Software: Cost: ISP Provides Firewall services but might want this in the future

***Priority 1 costs: $15K one time costs $27,600 Recurring (per year)***

**Priority 2:**

- Share Printer/Network Devices
- Color Printer (net Capable) Cost: $8K
- B&W Printer (net capable) Cost: $5K
- Network Operating System Cost: Need to Upgrade to Windows for Workgroups for all Clients. Need to Upgrade 80246 computer to 80486 {because of Priority 3, this will be a peer network, therefore the NOS will be included in the individual Machine's software packages} Cost: $480

***Priority 2 costs: $14K***

**Priority 3:**

- User-Managed/Administered Network
- Peer -to-Peer Network Decision: The cost of this decision is $480, and would be included if Priority 2 decision is made.

***Priority 3 costs: $480 (is included in Priority 2)***

**Priority 4:**

- Something Really Easy to Use
- Plan to support an In-House Training Program for Windows for Workgroups
- IT Person needs to be trained ($2400/1 week class)
- Help desk cost: Need a person to be trained ($2400/1 week class)
- We Plan to use a publication/Standard Operating Procedure to serve as the Help Desk

***Priority 4 costs: $4800 for training***

**Priority 5:**

- Round the Clock Operation
- Need to have a computer person as part of the duty section. Should consider getting a Pager and Cell Phone. The computer person needs to be able to restart the system and have ISP phone number available for trouble calls.

Under Future Requirements, I have Dial-Up networking, to support the Admiral when he is on the road. For this, I will need a laptop computer (for him), and a modem for one of the servers, with remote access service (RAS) installed. This will cost about $5K. I know he will want this capability if we can afford everything else.

# ROCA USER INFORMATION FORM

**User Name:** _______Admiral Boss_________________________

**User Location:**

**Building Number:** ___1________

**Floor:** ____1_______

**Room:** ___20________

**Location Sketch (Include Measurements):**

**User Equipment:**

**Computer Type** _____Pentium PC_______________

**Operating System** ___Windows 95______________

**Net Interface Card Required?** X Yes No

**Additional Devices: Printer** __Laser Jet 4___________ Network Printer
________________

**Is there a specific workgroup this user will be assigned to?** X Yes No
___Command_________

**Installed Applications:**
Wordperfect, Lotus 1,2,3, DbaseIV

---

**New Applications Required:**
Exchange Client

---

**New Computers Required?**
No

# ROCA USER INFORMATION FORM

**User Name:** _______Seaman Gray_________________________
**User Location:**
**Building Number:** ___2________
**Floor:** ____1_______
**Room:** ___2________

**Location Sketch (Include Measurements):**

**User Equipment:**

**Computer Type** _____PC80286_______________
**Operating System** ___MSDOS______________
**Net Interface Card Required?** X Yes No
**Additional Devices: Printer** __None___________ Network Printer
___Admin_____________
**Is there a specific workgroup this user will be assigned to?** X Yes No
___Admin_________

**Installed Applications:**
Wordperfect, Lotus 1,2,3, DbaseIV

---

**New Applications Required:**
Exchange Client

---

**New Computers Required?**
Yes…. Need to upgrade to 80486/Windows 95

# ROCA BUILDING INFORMATION FORM

## (Reproduce for Number of Floors in the Building – 1 each)

**Building Number:** _________1____________

**Number of Users in the Building**: ________20__________

**Number of Floors in the Building:** __________1_______

**Location and Dimensions of Wiring Closet for each Floor:** 10X10 Room 15

**Sketch a floor plan for each floor (include dimensions if possible). Include User Office and Wiring Closet
Locations**

**Are there hung ceilings or raised floors on this floor?** X Yes No

---

**Existing and Available Cable routes for this floor/building**: None

# ROCA BUILDING INFORMATION FORM

## (Reproduce for Number of Floors in the Building – 1 each)

**Building Number**: _________2____________

**Number of Users in the Building:** ________10__________

**Number of Floors in the Building:** __________1_______

**Location and dimensions of Wiring Closet for each floor**: 10X10 Room 12

**Sketch a floor plan for each floor (include dimensions if possible). Include User Office and Wiring Closet**
**Locations**

**Are there hung ceilings or raised floors on this floor**? X Yes No
No Raised Floors, but hung ceiling

---

**Existing and Available Cable routes for this floor/building:** None

# ROCA BUILDING-TO-BUILDING INFORMATION FORM

**For Building** ___1______ **to Building** ____2________

**Distance between buildings:** ___100 feet___________________________

**Description of terrain between buildings (include parking lots, roads, etc).**

Virgin soil, 1 road between

---

**Building-to-Building Sketch (including measurements):**

---

**Location of Connection Points for Each Building:**

Building 1 is in room 15, Building 2 in room 10

---

**Existing and Available routes for cable/Fiber**: None

# ROCA IN HOUSE SKILL LEVEL FORM

**Names and skill levels of personnel in the following disciplines:**

**Equipment Installation and Setup (include computer equipment and network equipment – NICS/Routers, etc):**

ET3 Smith has good skills in computer repair, and has installed a network at a previous command

**Network cabling Installation and Setup (include cable pulling, installation of wall jacks, etc):**

None

**Equipment and Network Maintenance (repair of network equipment):**

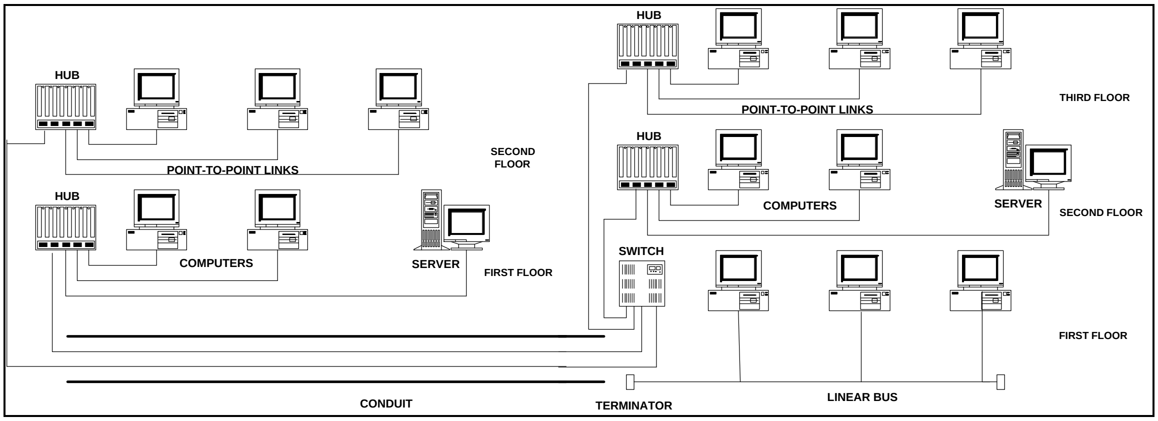
ET1 Webber has been to CISCO router maintenance school

**Network Management (administration and management of network operating system):**

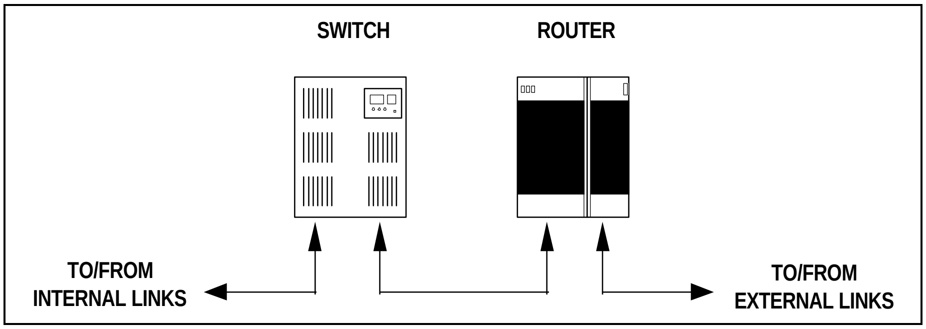
LT Jones has a computer science degree from Naval Postgraduate School

**Applications Experts (for help desk functions):**

Chief Simon is a guru on Wordperfect
YNSN Poholski knows Lotus 1,2,3
Ens Hardy knows Dbase IV



**Representative Inter-Building LAN Configuration.**



**Internal/External Link Connectivity.**

These two figures show inter-building and internal/external connectivity, which are two major areas in your network plan. Cut and paste these figures as required to come up with a good and annotated representation of your network.

## RULES OF THUMB FOR ESTIMATIONS

| **Router** |
|---|
| See the description of routers in the text. A basic cost for a good router is $18K. A FDDI network interface is $12K. An ATM network interface is $17K. A 6-port ethernet interface card is $12K. We recommend only using 5 out of the 6 ports. Keep the sixth one for a spare or for future growth. Prices, port configurations, numbers of slots available and capability vary greatly from company to company. The fewer the number of users, the higher the cost per user. If you know enough about your current situation, you can itemize, but a good rule of thumb for router cost is about $70/user. |

**Etherswitch**

The etherswitch is a network device that helps control loading on a network segment. The switch will not forward all traffic down all attached segments. It forwards only to the segment that the packet's destination device is attached. Costs vary based on capability and number of ports depends upon the manufacturer. The range is from $5K to $40K. Taking an average, 10 port switch, the cost per user is $85. With assignment:

- 6 ports for hub attachment
- 1 port for server attachment
- 1 port for router connection
- 2 ports for spares

**ATM Device**

If you are connecting to an ATM backbone, you may be required to purchase a switch (in some cases it might be included in the service, but you need to ask). You need to check the current market to determine the actual cost of a switch.

**Building Wiring**

This applies to the wiring inside the building. This is the hardware that goes from the wall plate to the central wiring closet(s). The number of wiring closets will depend upon the size and layout of a building. The components are:

- $50/user for miscellaneous connectors, wire, CAT5 cable, wall boxes, patch panels, patch panel rack, etc.

- $90/user for installation of the above. For both of these a minimum of 20 people is assumed. If you do this by 1s and 2s it can be a cost killer.

**Hubs**

This is for a 24-port SNMP manageable 10BaseT hub. This is based on connecting 20 people to a hub. The hub costs approximately $1200. Port use is as follows:

- 20 user ports
- 1 port for server
- 1 port for router
- 2 spares

$10 per user for a fully loaded hub. We recommend putting more hubs in for future growth. You can get hubs with 12, 24, 36, 48, etc. ports. From a network design perspective and to keep network loading down connecting a maximum of 20 people per hub is a good idea.

Consider $15-20/user for a 100BaseT Hub for estimation purposes.

**Physical Factors Cost Estimation**

Physical layer cost model - external plant, i.e. cable and conduit between buildings

Plant installation cost varies with the following factors:

**Distance -** a run with constant parameters (all other factors remain the same) will cost less per unit as the distance increases. As in any other endeavor, quantity brings the price down and this applies directly to conduit/cable installation.

**Building entries -** the number and complexity of the building entry is the most variable factor. This factor is highly variable because every building is different. New buildings generally have cable entry designed and built into the building where older buildings don't. Also the building structure has an effect on ease of entry. It is significantly less expensive to provide an opening in a wood framed building than it is in a concrete structure. Think of adding to a gun bunker in this case.

**Topology -** topology varies from virgin soil to a highly industrialized well traveled, street. In the first instance, it is just trenching through dirt and rock without any manmade obstacles where in the second case there would be existing conduits, pipes, roadway and sidewalks to contend with.

**Configuration -** the configuration can vary from a single direct buried cable to a multiple conduit bank with interduct and cable glides. Also the back fill involved can vary from just recovering with dirt to concrete slurry encasement with roadway/sidewalk repair.

Several communications installation companies were surveyed and the cost model reflects the general consensus of these companies. The model is based on a 4 inch conduit bundle with interduct and fiberglide covered with slurry. The statistical average cost is approximately $88 per lineal foot. The cost for virgin soil is $50 per foot with the maximum being $150 per foot for short runs into complex building entries. To provide a rough order of magnitude for estimation, a cost of $100 per foot can be used to reflect all factors relating to the Physical Factors Cost Estimation

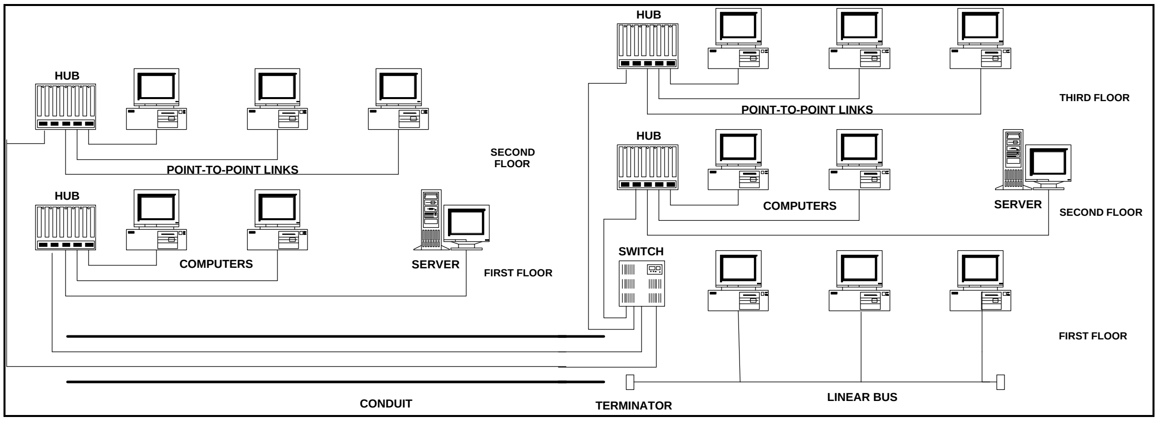
.

Congratulations, you now have enough rules of thumb to deal with for the real tough cost estimating. As with any rule of thumb, it provides an order of magnitude estimate that can be refined later.

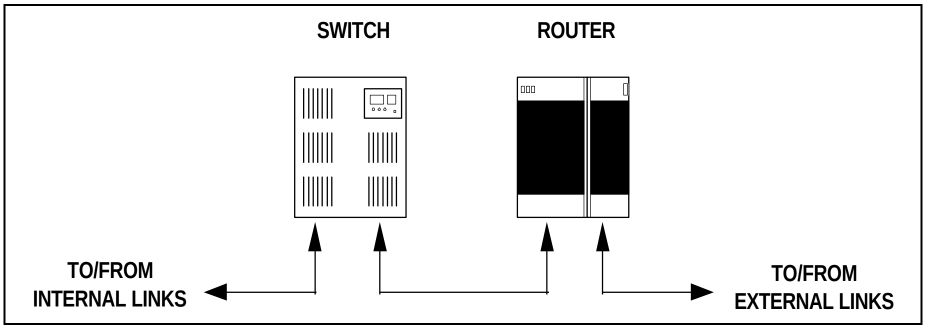
Armed with your ROCA user studies, you can put together some rough-cuts, refining your estimates as you iterate. Remember that these are just estimates. You will need to refine these estimates based upon gaining specific cost information from various sources. Section 4 of the Network Guidebook, and in particular Table 6, will give you resources and sources of information on existing contracts that will help you refine your estimates. You now have enough information to pursue this phase.

## Definition and Design Fill-Out Forms:

Figures 6 and 7 from the main document are included for your modification to fit your situation.



**Representative Inter-Building LAN Configuration.**



**Internal/External Link Connectivity.**

These two figures show inter-building and internal/external connectivity, which are two major areas in your network plan.

## <u>Thumb Rule Initial LAN Cost Estimate</u>

| Factor | Rate | Numbers | Total |
|---|---|---|---|
| Router | $70/User | 30 Users | $2100 |
| ATM device (if needed) | Market | Not Needed | |
| Building Wiring | $140/user | 30 Users | $4200 |
| Hubs | $20/user 100BaseT | 30 Users | $600 |
| Physical Factors | $100/foot | 100 Feet | $10,000 |
| Total this Table | | | $16,900 |

Other Cost Factors (additional Costs or Costing Refinement):

**Q 1. Would each person in the organization require a desktop computer?**

- **Q 2. How many desktop computers will be required?**
  - **a Itemize by building.**
- **Q 3. How many new desktop computers will be procured?**
  - **a) Itemize these.**
  - **b) Determine cost for these items.**
- **Q 4. How many NICs will be required?**
- **Q 5. What application software must be procured?**
  - **a) E-mail?**
  - **b) Web Browser?**
  - **c) File Transfer?**
- **Q 6. What supporting application hardware must be procured?**
  - **a) Mail server?**
  - **b) DNS host?**
  - **c) File server?**
- **Q 7. How would these computers be spread out in the area that the organization occupies?**
  - **a) Within a single building?**
  - **b) Within more than one building? How many?**
  - **c) What is the physical distance between each pair of buildings?**
  - **d) Do conduits exist for routing between buildings?**
- **Q 8. What are the relative distribution of users within each building?**
  - **a) Clustered?**
  - **b) Distributed?**
  - **c) Both?**
  - **d) Estimate of linear feet of media required.**
- **Q 9. Wall Jacks?**
- **Q10.-What supporting hardware will be required?**
  - **a) Switches**
    - **a) Port capacity**
  - **b) Routers**
    - **a) External**
    - **b) Internal**
  - **c) Hubs**

**Add these items which relate to additional costs to the previous thumb rule estimation and you will get a gross estimate of cost.**

**Cost of our Network ______________________**

**Cost Refinement and Specificity**

**Complete a wiring diagram before doing this**

## Cost Tabulation

| Item | Nomenclature | Quantity | Cost Per Item | Total Cost |
|---|---|---|---|---|
| 1. Computers | | | | |
| 2. NICs | | | | |
| 3. E-mail Software | | | | |
| 4. Web Browser | | | | |
| 5. File Transfer | | | | |
| 6. Mail Server | | | | |
| 7. File Server | | | | |
| 8. DNS Host | | | | |
| 9. Building Cable/Building: | | | | |
| a. Wall Plate to Wiring Closet | | | | |
| b. Computer to Wall Plate | | | | |
| c. Floor to Floor | | | | |
| 10. Building to Building Cabling | | | | |
| 11. Switches | | | | |
| 12. Routers | | | | |
| a. External | | | | |
| b. Internal | | | | |
| 13 Hubs | | | | |

| | |
|---|---|
| TOTAL COST | |

# APPENDIX E:

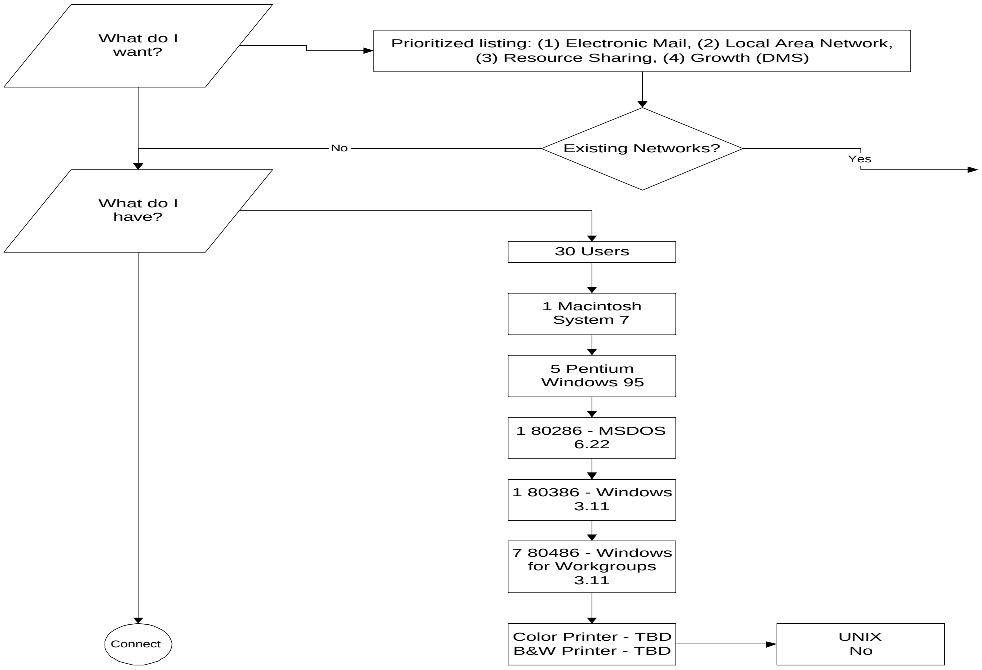
# PROCESS DATA FLOW DIAGRAMS

## FLOWCHARTS FOR USER EXPECTATIONS

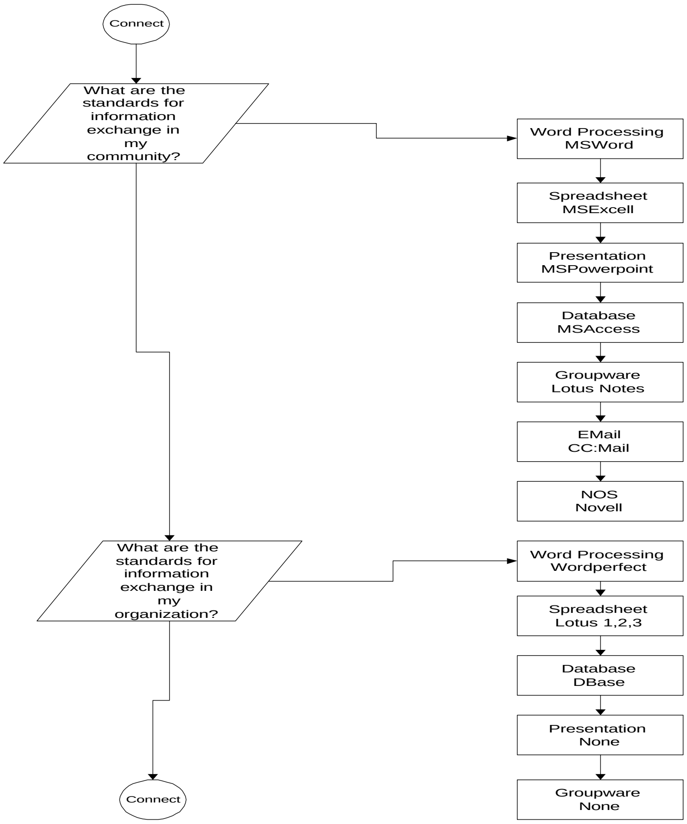
### User Expectations

Scenario Flowchart

Flag Aide for a 30 person staff. Admiral wants Electronic Mail. Additionally, we want to have 2 new network printers (1 color, 1 B&W). We have heard about DMS, how will this impact us?



# User Expectations (2)



Connect

What are the standards for information exchange in my community?

Word Processing MSWord

Spreadsheet MSExcell

Presentation MSPowerpoint

Database MSAccess

Groupware Lotus Notes

EMail CC:Mail

NOS Novell

What are the standards for information exchange in my organization?

Word Processing Wordperfect

Spreadsheet Lotus 1,2,3

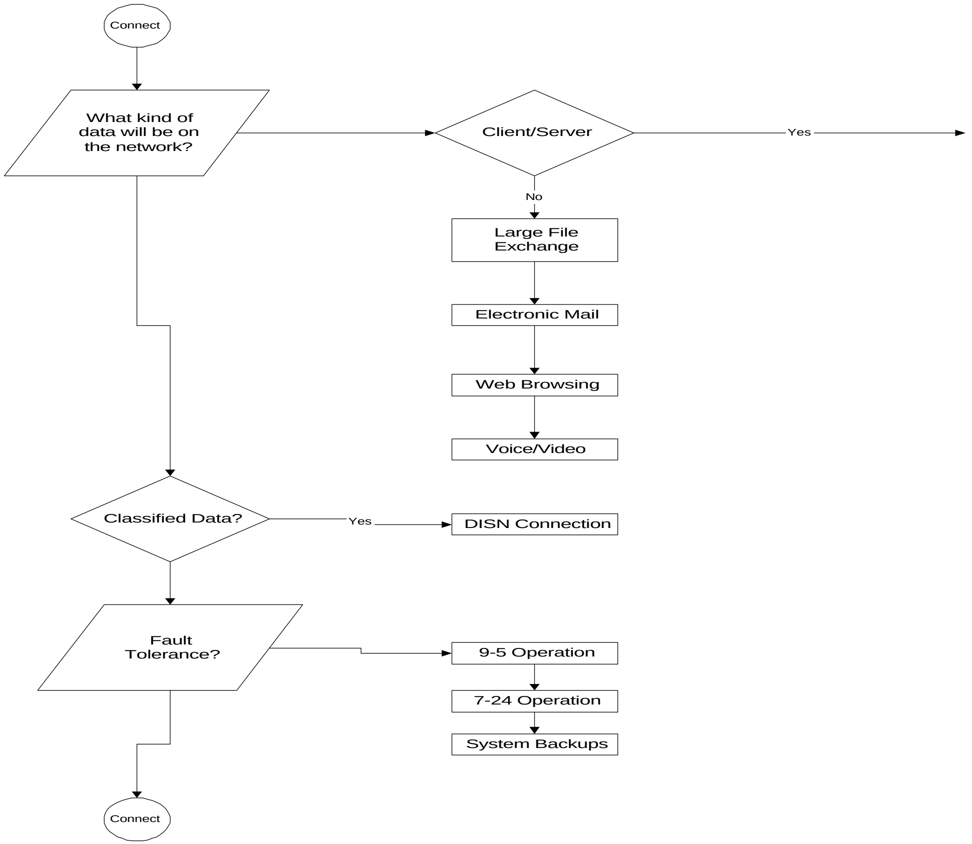
Database DBase

Presentation None

Groupware None

Connect

# User Expectations (3)



Connect

What kind of data will be on the network?

Client/Server

Yes

No

Large File Exchange

Electronic Mail

Web Browsing

Voice/Video

Classified Data?

Yes

DISN Connection

Fault Tolerance?

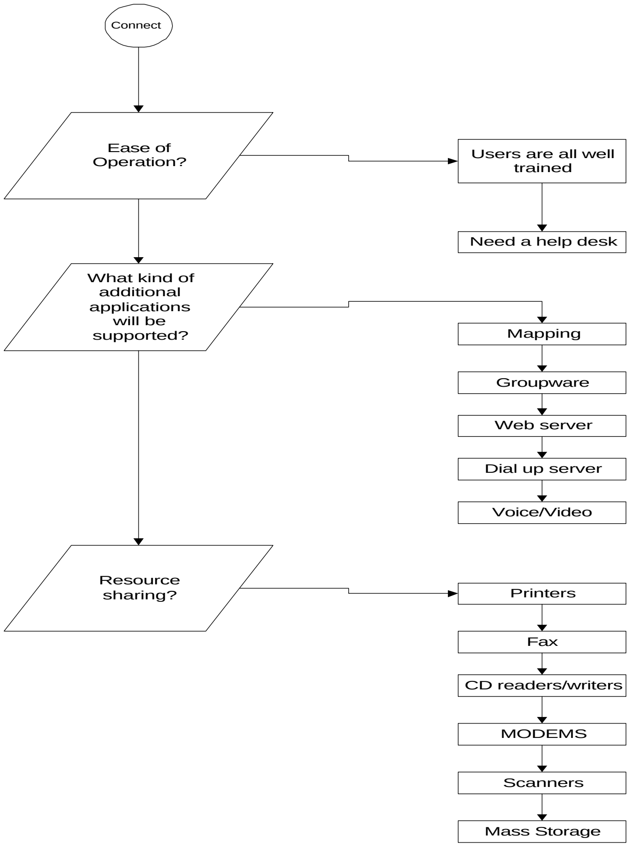
9-5 Operation

7-24 Operation

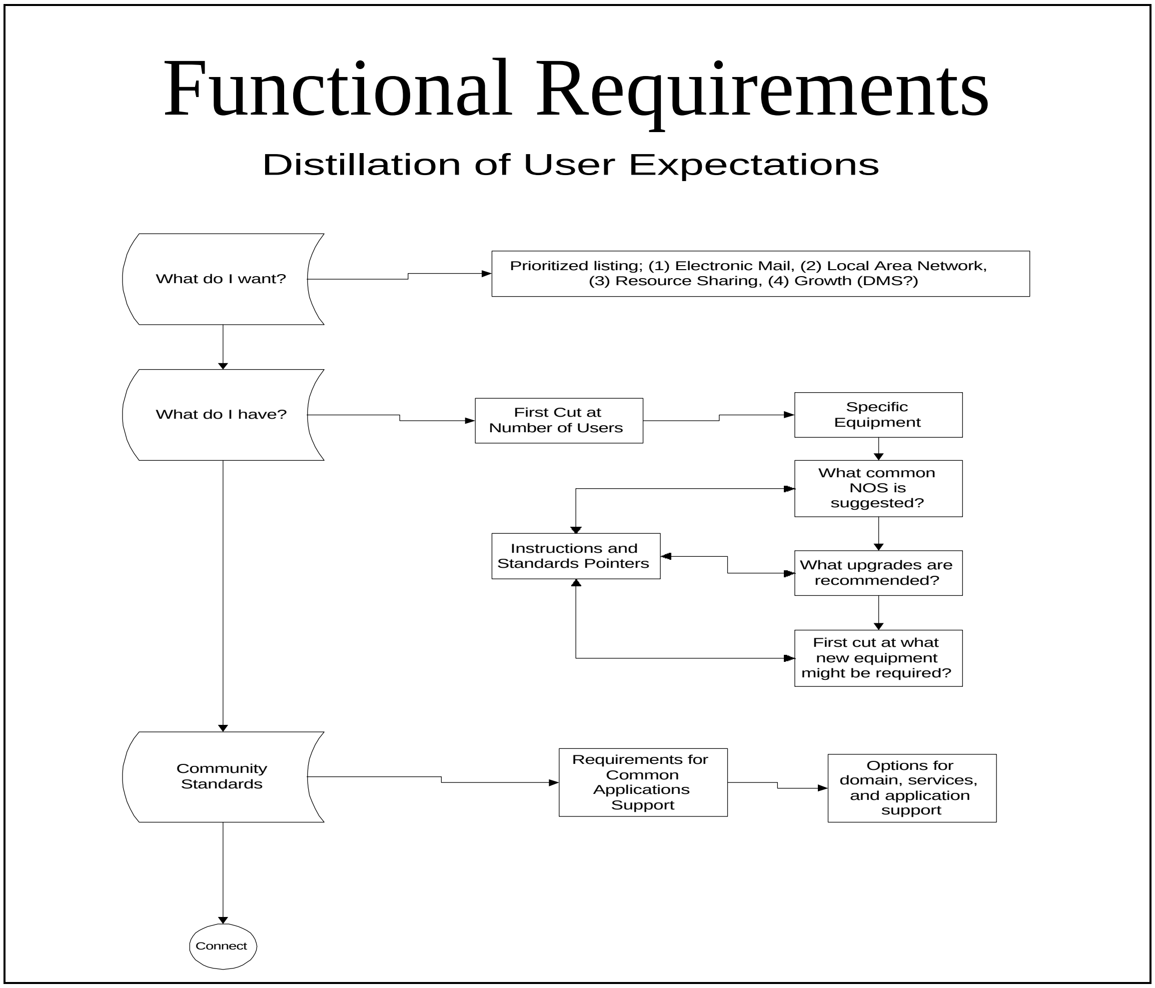
System Backups

Connect

# User Expectations (4)



## FUNCTIONAL REQUIREMENTS PROCESS FLOWCHARTS



# Functional Requirements

Distillation of User Expectations

What do I want?

Prioritized listing; (1) Electronic Mail, (2) Local Area Network, (3) Resource Sharing, (4) Growth (DMS?)

What do I have?

First Cut at Number of Users

Specific Equipment

What common NOS is suggested?

Instructions and Standards Pointers

What upgrades are recommended?

First cut at what new equipment might be required?

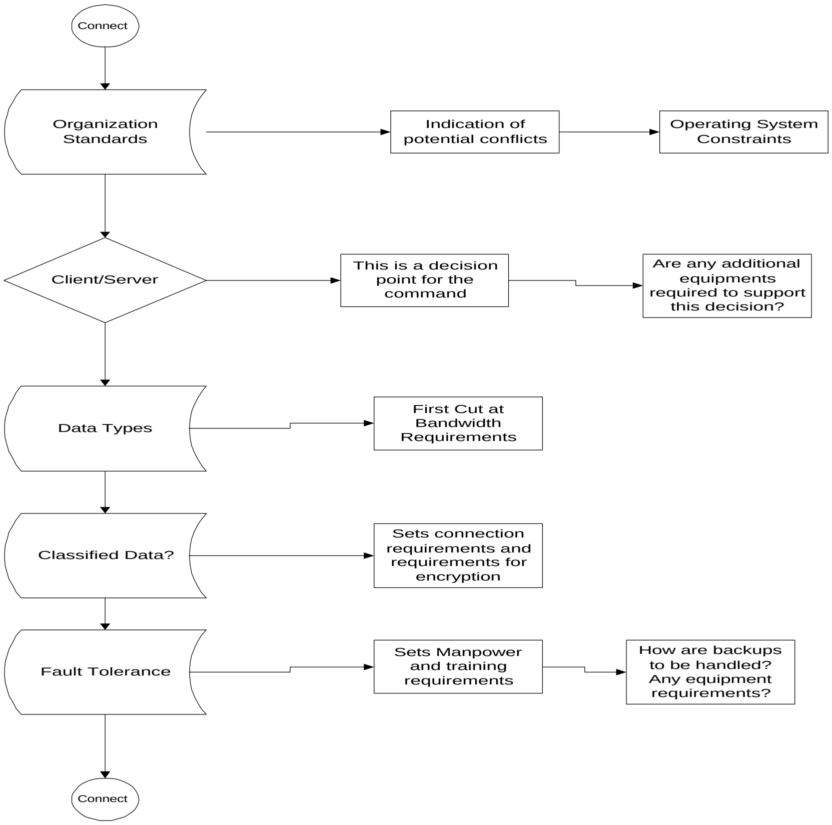
Community Standards

Requirements for Common Applications Support

Options for domain, services, and application support

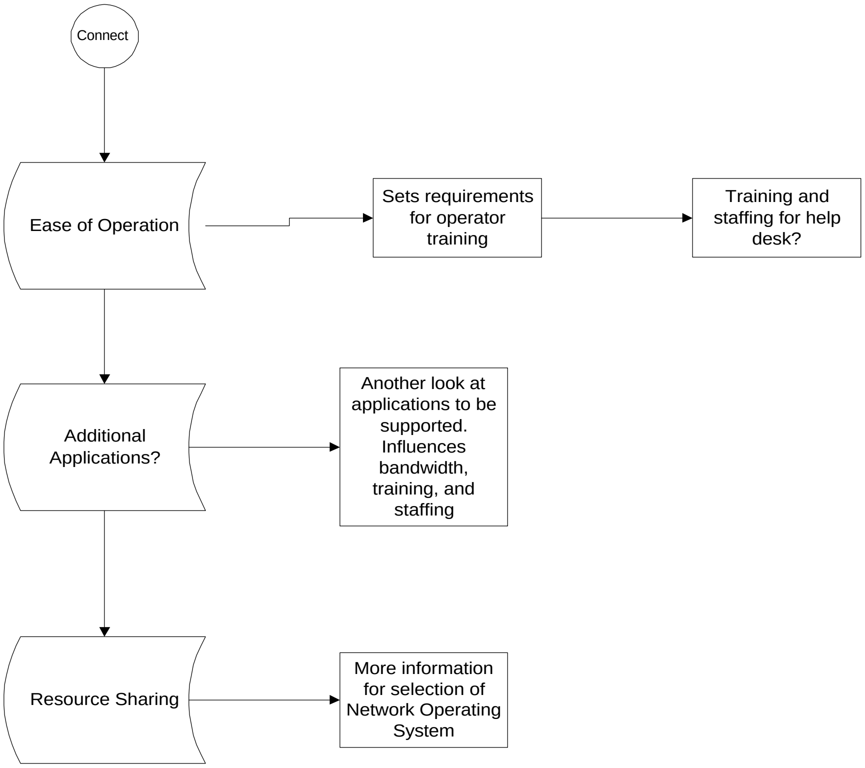
Connect

# Functional Requirements (2)



Connect
Organization Standards
Indication of potential conflicts
Operating System Constraints
Client/Server
This is a decision point for the command
Are any additional equipments required to support this decision?
Data Types
First Cut at Bandwidth Requirements
Classified Data?
Sets connection requirements and requirements for encryption
Fault Tolerance
Sets Manpower and training requirements
How are backups to be handled? Any equipment requirements?
Connect

# Functional Requirements (3)


Connect
Ease of Operation
Sets requirements for operator training
Training and staffing for help desk?
Additional Applications?
Another look at applications to be supported. Influences bandwidth, training, and staffing
Resource Sharing
More information for selection of Network Operating System

# Functional Requirements (4)

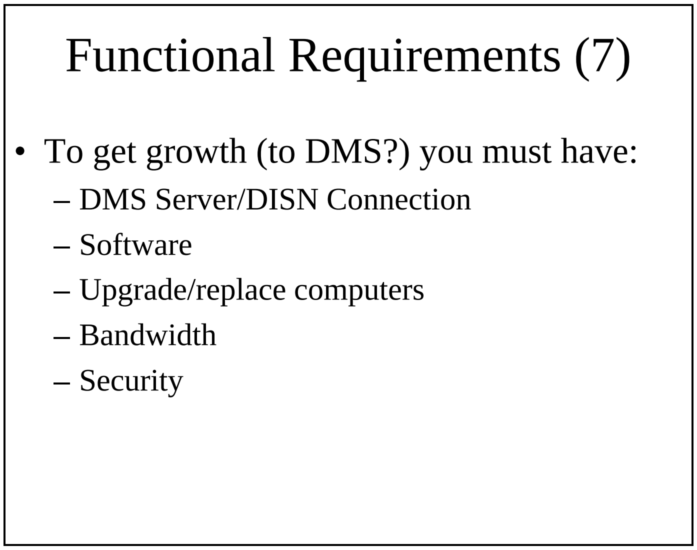
- To get Electronic Mail you must have:
  - External Internet Connection
  - Mail Server/Domain
  - Gateway (depends on mail software)
  - Software
    - Options (see Resources and Operating Conditions Assessment (ROCA))

## Functional Requirements (5)

- To Get LAN you must have:
  - – Cable Plant
  - – Network Interface Cards
  - – Hubbing/Routing
  - – Software

## Functional Requirements (6)

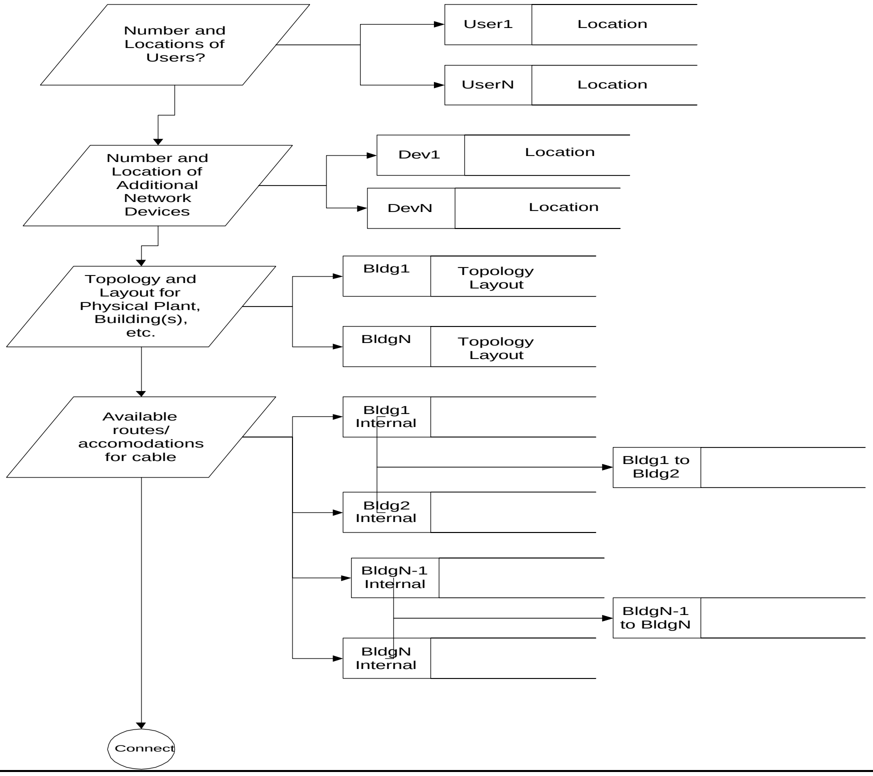
- To get Network Printing you must have:
  - – Network Capable Printer
  - – Network Printer Interface
  - – Resource Sharing
  - – Software



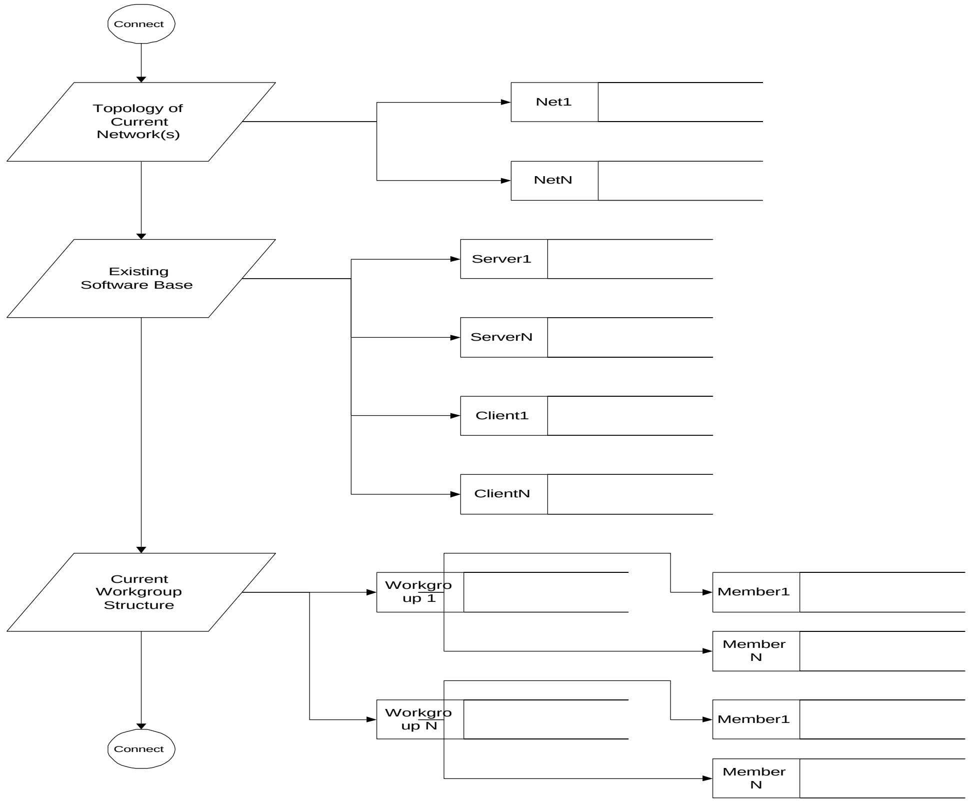
# Functional Requirements (7)

- To get growth (to DMS?) you must have:
  - – DMS Server/DISN Connection
  - – Software
  - – Upgrade/replace computers
  - – Bandwidth
  - – Security

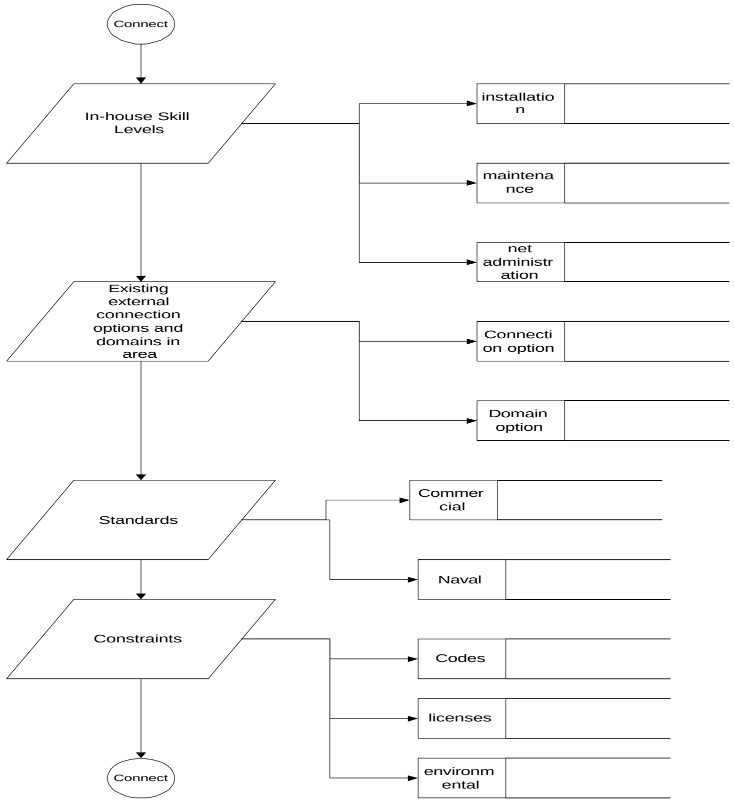
# Resources and Operating Conditions Assessment



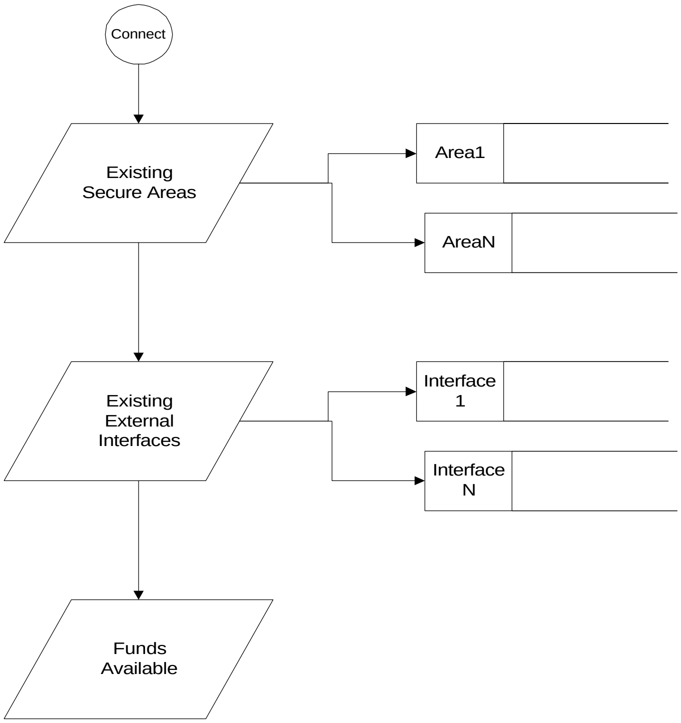
# Resources and Operating Conditions Assessment (2)



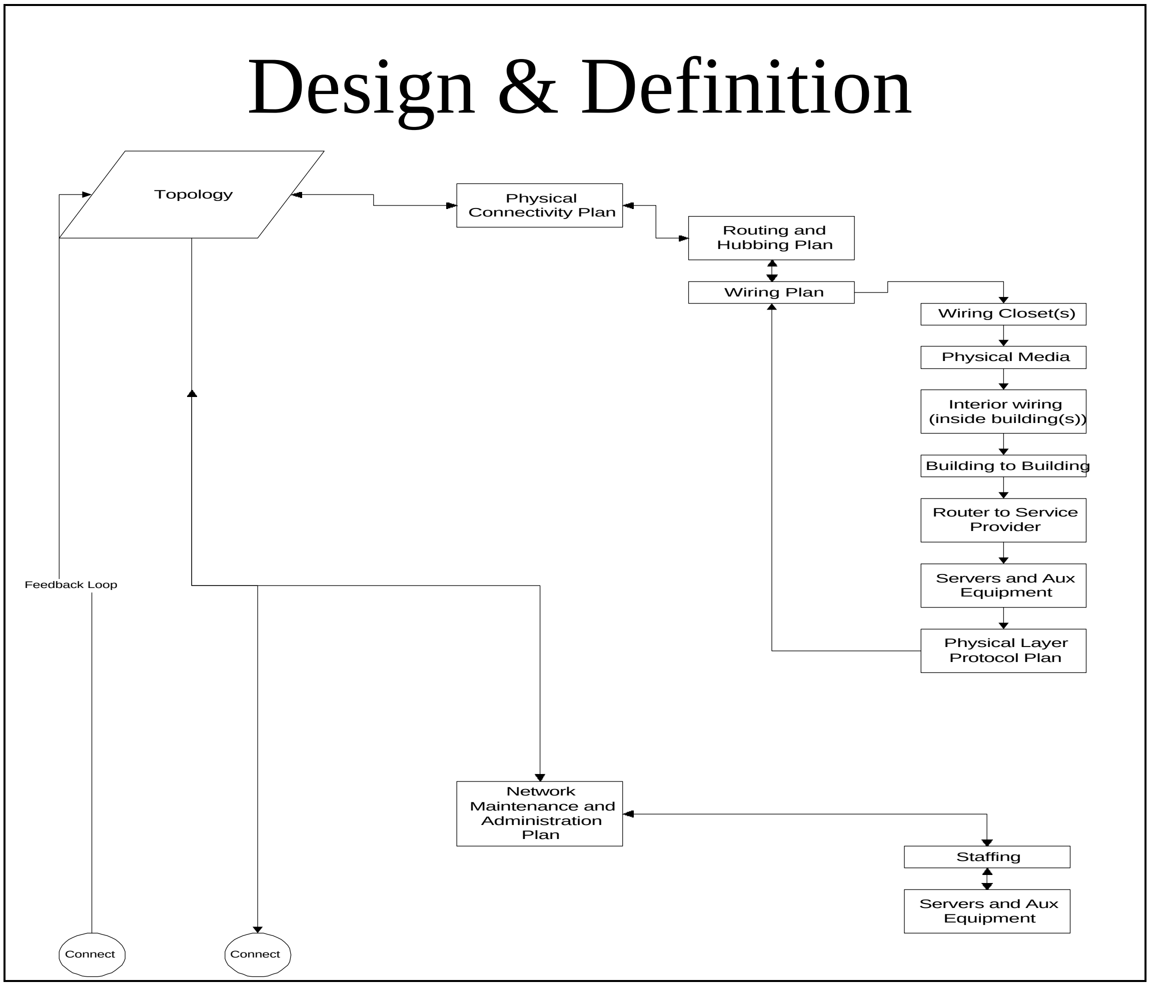
# Resources and Operating Conditions Assessment (3)



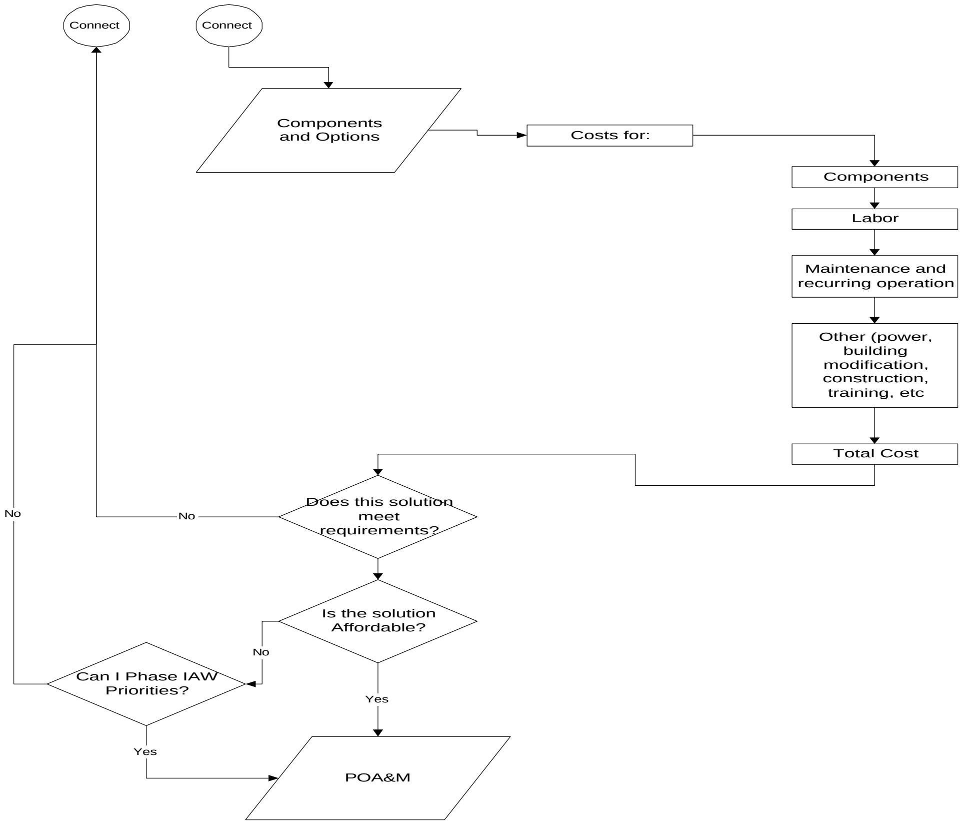
# Resources and Operating Conditions Assessment (4)



## DESIGN AND DEFINITION PROCESS FLOWCHARTS


Design & Definition
Topology
Physical Connectivity Plan
Routing and Hubbing Plan
Wiring Plan
Wiring Closet(s)
Physical Media
Interior wiring (inside building(s))
Building to Building
Router to Service Provider
Servers and Aux Equipment
Physical Layer Protocol Plan
Feedback Loop
Network Maintenance and Administration Plan
Staffing
Servers and Aux Equipment
Connect
Connect

# Design & Definition (2)



Connect

Connect

Components and Options

Costs for:

Components

Labor

Maintenance and recurring operation

Other (power, building modification, construction, training, etc

Total Cost

Does this solution meet requirements?

No

No

Is the solution Affordable?

No

Yes

Can I Phase IAW Priorities?

Yes

POA&M